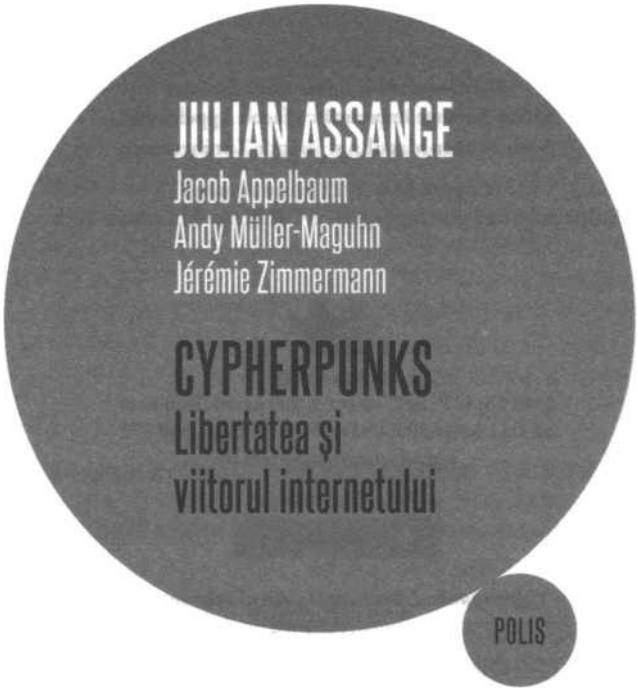
JULIAN ASSANGE
Jacob Appelbaum – Andy Miiller-Maguhn
CYPHERPUNKS Libirtitei; i viHirul iilerietilii

Julian Assange este redactorul-şef al Wikileaks, distins cu premiul „Noile Media” al Amnesty International (2009), premiul fundaţiei Sydney pentru pace (2011), premiul „Walkley” pentru jurnalism (2011) şi premiul „Martha Gellhorn” (2011). Unul dintre colaboratorii iniţiali la lista de e-mailuri cypherpunk, este creatorul a numeroase proiecte de software inspirate de filosofia cypherpunk, inclusiv al sistemului de fişiere Rubberhose pentru criptare şi al codului original pentru Wikileaks. A mai publicat cartea *Underground* (împreună cu Suelette Dreyfus, 2012), o istorie a mişcării internaţionale a hackerilor.



Traducere din limba engleză de VLADIMIR LAZURCA
Prefaţă la ediţia în limba română de CLAUDIU CRÂCIUN

Cypherpunks.
Freedom and the future of the Internet Julian Assange împreună cu Jacob Appelbaum.
Andy Müller-Maguhn şi Jérémie Zimmermann
Copyright © 2012 Julian Assange Ediţie publicată prin înţelegere cu OR Books LLC, New York

Editura Litera
O.P. 53; C.P. 212, sector 4, Bucureşti, România tel. 021 319 6390; 031 425 1619; 0752 548 372 e-mail: comenzilitera.ro
Ne puteţi vizita pe

Cypherpunks. Libertatea şi viitond internetului Julian Assange
Copyright © 2016 Grup Media Litera pentru versiunea în limba română Toate drepturile rezervate
Editor: Vidraşcu şi fiii
Redactori: Carmen Ştefania Neacşu, Mihaela Moroşanu Copertă: Flori Zahiu Tehnoredactare şi prepress: Anca Suciu
Descrierea CIP a Bibliotecii Naţionale a României ASSANGE, JULIAN
Cypherpunks. Libertatea şi viitorul internetului / Julian Assange; trad.: Vladimir Lazurca – Bucureşti: Litera, 2016
ISBN 978 – 606 – 33 – 0610 – 5 I. Lazurca, Vladimir (trad.)

Cuprins

Prefaţă la ediţia în limba română (Claudiu Crăciun) 7
Ce este un *cypherpunk*? 29
Introducere:
O chemare sub armele criptografice 31
Participanţii la discuţie 37
Nota editorului 40
Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei 41
Intensificarea comunicării *versus* intensificarea supravegherii 49
Militarizarea spaţiului cibernetic 61
Combaterea supravegherii totale cu ajutorul legilor omului 69
Spionajul sectorului privat 79
Combaterea supravegherii totale cu legile fizicii 87
Internetul şi politica 95
Internetul şi economia 113
Cenzura 137
Confidenţialitate pentru cei slabi, transparenţă pentru cei puternici 163
Şobolanii de la Operă 171
Note 183

Prefaţă la ediţia în limba română[1]

I *t*

Numele lui Julian Assange nu este foarte cunoscut în România. Al partenerilor lui de dialog, cu atât mai puţin. Doar cei interesaţi de politica internaţională, de dezvoltarea tehnologiei informaţiei sau de drepturile fundamentale sunt familiarizaţi cu persoana sa şi cu odiseea lui legală. Dar incomparabil mai mulţi cunosc şi

1 Lc sunt recunoscător lui Constantin Vică, Daniel Cernat şi Nicoletei Andreescu pentru comentariile şi sugestiile asupra textului.

chiar folosesc platformele şi tehnologiile pe care Assange şi colegii lui le analizează critic în cartea de faţă. Google, Facebook, Twitter, Amazon, Microsoft, Apple. Sunt companiile din avangarda tehnologiei informaţiei şi cele care au preluat internetul, îl structurează şi, odată cu el, comunicaţiile tuturor. Pe lângă faptul că sunt branduri influente, au putere economică, juridică şi politică, iar aceasta creşte exponenţial. Cooperează cu guvernele, formând un complex tehnologico-informaţional care deţine controlul asupra interacţiunilor dintre miliarde de oameni. Perspectiva este ameţitoare: miliarde de oameni angrenaţi în comunicare şi schimburi şi care produc urme vizibile şi stocabile; întreaga istorie a umanităţii, de la cea individuală la cea macrosocială, se reflectă în uriaşe centre de date. Iar de acolo, companiile private şi guvernele extrag informaţii despre oricine şi despre toţi, devenind proprietarele unui tezaur de cunoaştere care le oferă o putere şi o independenţă unice în istorie.

Problema fundamentală a internetului, cel puţin aşa cum o văd Assange şi colegii lui, este faptul că o întreagă civilizaţie s-a mutat în virtual, iar acest spaţiu, din cauza tehnologiei de supraveghere, devine unul distopic, din care nu mai putem refuza să facem parte, dar asupra căruia nu mai exercităm niciun control. Avem de ales între a ne izola, refuzând participarea la interacţiunea socială, şi a ne preda sfera privată şi datele companiilor şi guvernelor. Cypherpunks ne prezintă acest spectru, neliniştitor în întregul lui, cu scopul de a ghida o participare conştientă, responsabilă, protejată şi descentralizată la spaţiul virtual.

Volumul redă de fapt un dialog între membrii unei comunităţi mult mai largi şi redutabile de specialişti în tehnologia informaţiei, activişti, jurnalişti şi analişti ai internetului. Scopul lor asumat este limitarea puterii

companiilor şi guvernelor, dezvăluirea secretelor de interes public şi protejarea intimităţii din ce în ce mai fragile a cetăţenilor, prizonieri benevoli ai internetului. Dialogul lor, dens şi viu, nu este însă unul tehnic, un schimb între specialişti ai hardware-ului şi ai software-ului. Este unul în care istoria, geografia, ideile, puterea şi politica se întrepătrund cu tehnologia. Exact această întrepătrundere şi interdependenţă fac dialogul semnificativ. Tehnologia nu constituie o sferă izolată, ci este inclusă în societate, transformând-o la fiecare pas. Direcţiile transformării pot fi problematice, pentru că orice tehnologie poate fi folosită şi în scop constructiv, şi în scop distructiv. Această ambivalenţă este prezentă şi în acest caz. Astfel, a privi răspândirea tehnologiei informaţiei ca fiind ceva inerent bun este un optimism care poate înşela. Tehnologiile nu produc în mod automat bunăstare, siguranţă, sănătate, democraţie şi egalitate, mai ales atunci când se află în posesia unui grup restrâns sau când devin arme în mâinile unor organizaţii ori guverne. Tehnologia este parte a puterii, pe care o constituie şi o conservă. Iar puterea exclude şi include, divide sau uneşte, distruge sau construieşte, favorizează sau discriminează.

Tiparul şi cartea scrisă, mijloacele moderne de transport, electricitatea, telefonia, radioul şi televiziunea au schimbat cursul istoriei. Efectele internetului asupra civilizaţiei sunt la fel de puternice ca ale acestor tehnologii, dar, spre deosebire de acestea, care au avansat modular, inegal şi într-un timp îndelungat, internetul cuprinde întreaga omenire într-un ritm extrem de rapid. Dialogul dintre cei patru autori arată că tehnologia informaţiei şi comunicaţiilor schimbă tot – felul în care interacţionăm şi chiar cel în care percepem realitatea. Numărul celor care deţin dispozitive pentru conectarea la

internet e în creştere exponenţială. Telefoanele devin din ce în ce mai sofisticate, preluând funcţiile PC-urilor. Cu ajutorul dispozitivelor electronice şi al internetului, de la cele mai fragede vârste oamenii se informează, se educă, comunică, se distrează, cumpără şi vând, îşi găsesc parteneri, îşi evaluează sănătatea, caută mijloace de transport, controlează aplicaţii şi aparatele electrocasnice. Aşa-numitul Internet al lucrurilor creşte conectivitatea cu tot ceea ce ne înconjoară şi ne este de folos, în fiecare zi devenim tot mai conectaţi şi mai dependenţi de tehnologie şi internet. Iar această conectare lasă urme, arătând unde suntem, cu cine suntem, ce consumăm, ce ne place şi ce nu ne place, ce stil de viaţă avem, cât de sănătoşi sau de mobili suntem, cât de populari sau deprimaţi suntem. Fiecare aspect al vieţii noastre, fiecare alegere, fiecare gest lasă o urmă digitală, stocată undeva. Prin simplul fapt că existăm digital, producem informaţie şi devenim o ţintă pentru cei interesaţi de respectivele informaţii. Interesul este economic pentru companii şi politic pentru guverne. împreună, acestea colaborează pentru a produce, stoca şi analiza mai bine datele existenţei noastre. Programele de supraveghere şi spionaj se banalizează, înregistrarea comunicaţiilor la fel. Programele de recunoaştere a vocii şi a trăsăturilor faciale devin din ce în ce mai performante. Pare că vocaţia inovaţiei tehnologice actuale este creşterea „lizibilităţii” comportamentului uman în toate aspectele acestuia. Iar această citire şi ordonarea comportamentului uman individual devin imperativul guvernării şi al economiei.

Protecţia datelor personale şi a comunicaţiilor private este în principiu garantată constituţional, cel puţin în democraţiile liberale. Există o cultură a protejării datelor cu caracter personal, mai ales în Europa şi în

America de Nord, unde orice intruziune trebuie justificată şi validată legal, şi numai în relaţie cu o faptă ilegală în privinţa căreia există dovezi anterioare. Adică cei cărora li se ascultă telefoanele sau cărora li se citeşte poşta electronică sunt persoane care au comis sau urmează să comită o infracţiune. Limitarea drepturilor poate fi în principiu justificată, iar aceste limitări sunt prevăzute în legislaţie şi validate de un judecător, independent de activitatea organelor de anchetă. Aceste proceduri au fost însă cu totul depăşite de viteza cu care se dezvoltă tehnologia şi de libertatea de facto pe care serviciile de informaţii şi cele poliţieneşti au căpătat-o inclusiv în democraţiile occidentale. Modelul dominant a devenit cel în care toate comunicaţiile sunt supravegheate şi înregistrate în masă, şi abia apoi analizate de diferite agenţii pentru a afla informaţii relevante despre anumite persoane şi grupuri (ceea ce Julian Assange numeşte interceptare strategică).

Stat, tehnologie şi supraveghere

Contemplăm astăzi lumea nouă a comunicării şi accesului la informaţii şi putem avea iluzia unui sentiment de libertate. Idealiştii internetului timpuriu îl vedeau ca pe un instrument al cunoaşterii şi educaţiei, liber şi autoguvernat, lipsit de obstacole şi coerciţie. Istoria recentă l-a dus însă în alte direcţii. În primul rând, marile corporaţii au ajuns să îl domine. În al doilea rând, statele şi-au extins monopolul asupra constrângerii şi în acest spaţiu, folosind acest monopol pentru a-şi consolida puterea în lumea reală. Să devină oare internetul, dintr-o utopie a cunoaşterii, un coşmar al profitului şi supravegherii? Cei care au participat la acest dialog, şi nu numai ei, asta cred. Este important să vedem cum s-a ajuns aici.

Statul a fost şi a rămas principalul motor al dezvoltării tehnologice. Fără sprijinul lui direct, principalele realizări tehnologice moderne nu s-ar fi putut răspândi. Statul a construit căi ferate şi le-a folosit pentru transport, comerţ şi război. A construit reţele electrice, drumuri şi autostrăzi. Atunci când tehnologiile trebuiau transferate în infrastructuri fizice, statul era acolo, prin investiţii, aprobări, legiferare, control, impozitare, servicii de urgenţă. Există o prezenţă variabilă, dar puternică a statului în operarea tuturor infrastructurilor, iar cele de importanţă majoră sunt direct controlate de acesta. Tehnologia comunicaţiilor şi internetul au însă o traiectorie diferită. Spre deosebire de alte domenii, statul nu mai este, în aceste cazuri, motor al dezvoltării şi/sau proprietar al infrastructurilor. Acestea sunt private. Terminalele şi dispozitivele, cablurile de reţea, centrele de date, capacităţile de stocare sunt private. Expertiza umană este concentrată masiv în zona privată. Acest lucru pune statele într-o poziţie dificilă în raport cu alte situaţii istorice, în care relaţia de autoritate era clară. De asemenea, pune companiile private într-o postură delicată, pentru că în principiu au datoria să îşi protejeze clienţii1. În practică, relaţia funcţionează mult mai bine decât se poate anticipa. În ţările autoritare, precum China, nu se poate pune problema protejării informaţiilor private. Probabil nici în ţări cvasiautoritare precum Rusia. Relaţia este însă mai interesantă în SUA, care sunt singura superputere globală şi, în acelaşi timp, ţara cu cei mai puternici jucători pe piaţa serviciilor şi produselor online. Fuziunea dintre interesele, resursele şi viziunea marilor giganţi ai internetului şi guvernul american pare completă2. Guvernul are acces direct la tot ce trece prin serverele acestor giganţi, aşa cum a dezvăluit contractorul NSA

Edward Snowden3. Şefii marilor corporaţii sunt activi în diplomaţia economică şi culturală americană4. Aceste corporaţii, dincolo de profiturile uriaşe pe care le extrag, răspândesc în lume idei, valori şi simboluri ce legitimează poziţia dominantă a Statelor Unite în lume.

Puterea statală a fost întotdeauna suspicioasă cu supuşii şi ulterior cetăţenii săi. Un bun conducător, un regim politic responsabil trebuie să ştie ce gândesc şi fac membrii comunităţii. Dar unde se află graniţa dintre guvernarea binevoitoare şi luminată şi controlul asupra societăţii? Democratizarea presupune creşterea controlului cetăţenesc asupra puterii politice. În acelaşi timp, statul îşi dezvoltă infrastructura guvernării, care este folosită atât pentru administrare, cât şi pentru control. Supravegherea guvernamentală, cel puţin în Europa, are o istorie lungă. Multă vreme, un stat eficient a fost acela care ştia exact unde îi locuiau cetăţenii, ce fel de proprietăţi aveau, ce fel de activităţi economice întreprindeau5 – pentru a-i impozita sau trimite la război. Cu timpul, instituţiile poliţieneşti, judiciare şi carcerale s-au întărit, atât în democraţii, cât şi în regimurile despotice şi autoritare6. Supravegherea în lipsa tehnologiilor actuale fiind o activitate costisitoare şi intensă, în trecut aparatele poliţieneşti trebuiau să se bazeze pe informatori şi delaţiune, pe un aparat birocratic masiv care să întreţină un sistem de strângere, arhivare şi analiză a informaţiilor. Pe rând, toate mijloacele de comunicare au fost interceptate – poşta fizică, transmisiunile radio, conversaţiile telefonice. Chiar înainte de apariţia internetului, statele erau prin urmare capabile să supravegheze la scară extinsă. Vârful acestei tendinţe de monitorizare şi control a fost statul totalitar, cel care, pe lângă ingineria socială violentă, a avansat cel mai departe

în controlul total asupra indivizilor. Doar limitele tehnologice au împiedicat statele să reuşească supravegherea deplină.

Arhitectura politică a supravegherii a fost concepută în timpul Războiului Rece, iar monitorizarea internetului astăzi este o extensie a acesteia într-un nou spaţiu. În primul rând, supravegherea este considerată o tactică de război, deci o chestiune de siguranţă naţională, justificând militarizarea şi generalizarea acesteia. În al doilea rând, supravegherea este în mod egal ţintită asupra adversarului şi a propriilor cetăţeni, aceştia din urmă fiind cu toţii suspectaţi că nu ar fi loiali regimului, ci unei forţe străine. În al treilea rând, supravegherea trebuie să fie globală, pentru că războiul este la fel. Nicio naţiune şi niciun cetăţean ai lumii nu se pot extrage din acest război. Statele Unite ale Americii şi Uniunea Sovietică au concurat în aceeaşi logică, aparatele lor de spionaj şi supraveghere răspândindu-se peste tot în lume, dar fiind în cele din urmă orientate cu precădere către interiorul respectivelor state. Ascultarea telefoanelor, urmărirea, interceptarea conversaţiilor din anii 1950 şi 1960 din America sunt un exemplu. Ulterior, SUA şi-au dezvoltat sisteme de supraveghere sofisticate. Uniunea Sovietică, un stat autoritar, şi-a dezvoltat la rândul său infrastructura de supraveghere pentru identificarea disidenţilor şi menţinerea regimului politic. Ca şi în cursa tehnologică de război propriu-zisă, Statele Unite au avut şi aici un avans tehnologic clar.

Sfârşitul Războiului Rece a detensionat parţial situaţia, dar nu a schimbat-o fundamental. Dezarmarea care a urmat a ţintit arsenalul nuclear şi pe cel convenţional, şi nu infrastructura de comunicaţii, respectiv de supraveghere. La zece ani de la sfârşitul Războiului

Rece a apărut însă un nou tip de conflict, cel cu terorismul islamist, ca răspuns la atentatele asupra turnurilor gemene din New York şi a Pentagonului din 20017. Din nou, vorbim despre o problemă globală ce are ramificaţii în interior, deci supravegherea trebuie să îi urmeze. Transferul gândirii de tip Război Rece către noua ameninţare s-a petrecut rapid. Rusia, de asemenea, a făcut transferul după atentatele de la Moscova (2002) şi Beslan (2004). Rivalitatea geopolitică a părut pentru moment amorţită şi înlocuită de lupta comună antiteroristă. Europa a făcut la rândul ei acest transfer, dar cu rezerve, chiar dacă se confruntase anterior cu incidente teroriste serioase, separatist-naţionaliste sau ideologice. Însă atentatele de la Madrid (2004) şi de la Londra (2005) şi, recent, cele de la Paris (noiembrie 2015) şi Bruxelles (aprilie 2016) par că o împing către militarizarea acestui conflict şi susţinerea supravegherii extinse pe care o presupune8.

Perioada post-Război Rece coincide cu răspândirea internetului. Monitorizarea şi militarizarea lui erau doar o chestiune de timp. Prin faptul că cetăţenii îl folosesc în mod voluntar, se rezolvă o mare şi persistentă problemă a statelor. Informaţia devine disponibilă imediat ce deschizi un program de navigare pe web sau apelezi pe cineva de pe telefonul mobil. Ceea ce părea cândva o imposibilitate devine acum realitate. Iar acest proiect nu este nici măcar un secret. Programul Total Information Awareness (TIA) îşi propune nici mai mult, nici mai puţin decât supravegherea totală. Datorită creşterii capacităţilor de stocare, este posibil ca un asemenea proiect să fie susţinut de bugetul unei singure ţări, în cazul de faţă SUA. Globalizarea părea că le-a răpit statelor din autonomie şi le-a limitat setul de instrumente pe care îl au la dispoziţie. Contrar acestei perspective, cel puţin în domeniul securităţii şi al

informaţiei, datorită inerţiei, războaielor şi internetului, ele devin, dimpotrivă, şi mai puternice.

Internetul şi democraţia

Impactul tehnologiei asupra procesului guvernării este major. Acest lucru este valabil atât pentru ţările democratice şi pentru cele nedemocratice, cât şi pentru cele în tranziţie de la o categorie la cealaltă. Tehnologia informaţiei şi internetul devin factori de accelerare sau de temperare a unor tendinţe istorice, fie că ne referim la transferul ideilor revoluţionare de la o societate la alta, fie la mobilizarea sau reprimarea mişcărilor de opoziţie. În dialogul din volum, tema democraţiei şi a democratizării este tratată pasager, perspectiva dominantă fiind aceea că tipul de regim nu contează, atât democraţiile, cât şi non-democraţiile fiind structural asemănătoare, având lin fel de ADN comun, bazat pe penetrarea totală a sferei private şi pe controlul interacţiunilor sociale mediate digital. În plus, se desprinde imaginea unor Leviatani, state concurente sau aliate care îşi dispută puterea la nivel global, dar a căror trăsătură comună este controlul cvasitotal asupra propriilor cetăţeni. În această lume nouă democraţia nu există, fiind transformată într-un joc electoral superficial, la vârful unei piramide a puterii în care blocurile sunt constituite din servicii de informaţii, birocraţii opace şi corporaţii puternice, cele care gestionează datele tuturor.

Este o imagine total contrastantă faţă de cea triumfalistă a victoriei democraţiei liberale asupra tuturor celorlalte forme de guvernare, răspândită după încheierea Războiului Rece. De asemenea, este o imagine total contrastantă faţă de cea a internetului şi a tehnologiei informaţiei ca principali aliaţi ai mişcărilor de opoziţie ce luptă pentru democratizare. De ce unele state se democratizează şi altele nu, de ce unele democraţii rezistă

şi altele nu, care sunt factorii şi mecanismele ce favorizează democraţia sunt întrebări care preocupă ştiinţa politică. Fără a detalia răspunsurile posibile, foarte numeroase şi deseori contradictorii, ne putem rezuma la o definiţie minimală a democratizării drept proces istoric de constrângere şi limitare a puterii politice prin intermediul legilor, al instituţiilor reprezentative şi al participării electorale extinse. Astfel, puterea politică este legitimă, inclusiv sub aspectul utilizării coerciţiei, numai dacă este investită de către cetăţeni prin vot şi numai dacă procesul alegerii şi al guvernării propriu-zise se supune unor reguli constituţionale care trasează clar limitele puterii şi responsabilităţii. În modernitate, acest proces a presupus centralizarea puterii de către principi şi apoi limitarea puterii acestora de către birocraţii publice şi adunări parlamentare alese în mod direct. Mecanismele ce fac democraţia să funcţioneze sunt cele prin care drepturile şi libertăţile individuale sunt protejate, participarea politică a cetăţenilor este încurajată, câştigarea şi pierderea puterii se fac în mod paşnic, prin alegeri, iar puterea, în momentul în care este câştigată, nu este folosită împotriva opoziţiei sau a grupurilor minoritare. Firul roşu al tuturor acestor mecanisme şi proceduri democratice este unul simplu: numai cei aleşi în mod direct pot conduce o societate democratică. Acolo unde societatea este condusă de către persoane care nu au fost alese prin vot, precum regii sau principii, sau de către persoane făcând parte din corpuri speciale precum clerul sau armata, nu poate fi vorba despre o democraţie. Democraţia reprezintă o stare de echilibru între instituţii şi grupuri sociale, deseori fragil, inclusiv în cadrul a ceea ce numim democraţii consolidate. Cel mai frecvent dezechilibru – şi cel mai important – este cel dintre stat şi societate. Atunci când asimetria de putere

dintre acestea creşte, democraţia e în pericol.

Ce impact au tehnologia informaţiei şi internetul asupra regimurilor autoritare? Aparent, le slăbesc, aşa cum am văzut în cazul Primăverii Arabe, când internetul a fost indispensabil mobilizării opoziţiei. Internetul are un rol antemergător important – cu ajutorul său circulă idei, argumente şi simboluri care pot eroda susţinerea regimurilor autoritare. Importanţa internetului este relevată şi de atenţia pe care o acordă autorităţile limitării accesului şi cenzurii. Resurse importante sunt dedicate acestor activităţi. În cazurile în care mişcările de opoziţie nu reuşesc îndepărtarea regimului autoritar respectiv, folosirea internetului are efectul invers, de slăbire a opoziţiei. Acest lucru se întâmplă pentru că opozanţii îşi dezvăluie public poziţiile şi tacticile şi devin ţinte ale represiunii. Aşadar, internetul poate fi un instrument eficient al opoziţiei, dar numai în măsura în care aceasta este foarte puternică, iar regimul autoritar, prea slab pentru a organiza represiunea. Tehnologia şi informaţia ajută, dar nu pot transforma structura socială şi raporturile de putere existente, cel puţin pe termen scurt. Dacă nu există o anumită configuraţie de forţe, interne şi externe, contestarea şi îndepărtarea regimurilor autoritare nu pot avea loc. Iar dacă acestea reuşesc să îşi construiască infrastructura necesară supravegherii totale, schimbarea de regim devine foarte dificilă.

Tehnologia informaţiei şi internetul funcţionează ca acceleratori ai tendinţelor autoritare, mai ales atunci când societatea respectivă este confruntată cu un duşman extern sau intern, real sau imaginat. Regimurile autoritare au inclusă în structura lor nevoia de duşmani, necesari pentru a putea menţine unitatea în timpuri de criză sau atunci când performanţele regimului nu îi asigură acestuia

legitimarea populară. Duşmanii interni iau forma unor minorităţi religioase, etnice sau lingvistice, a mişcărilor de opoziţie, a organizaţiilor nonguvernamentale sau a mass-mediei. Duşmanii externi sunt vecini sau puteri regionale ori globale. Supravegherea extinsă este justificată prin nevoia de a cunoaşte şi combate inamicii ordinii şi unităţii naţionale. În cazul în care unele dintre grupuri aleg calea rezistenţei armate, situaţia este definită ca un război şi tratată ca atare. Mai mult, regimurile autoritare realizează un transfer. Grupurile de opoziţie, oricare ar fi natura opoziţiei acestora, sunt tratate ca un întreg, şi instrumentele de represiune sunt transferate de la un grup la altul, de obicei de la cel mai periculos şi violent către cele mai paşnice. Retorica, supravegherea, intimidarea, represiunea sunt folosite şi împotriva luptătorilor, dacă există, şi împotriva opoziţiei politice paşnice. Ca exemplu, guvernul turc condus de Recep Tayyip Erdogan amestecă opoziţia politică, presa şi grupările armate, folosind lupta antiteroristă ca justificare pentru represiunea tuturor grupurilor de opoziţie.

În schimb, relaţia dintre tehnologia informaţiei, internet şi democraţii pare complementară. Datorită internetului, cetăţenii devin mai bine informaţi, interacţionează mai uşor, inclusiv din punct de vedere politic9. Internetul este noua locaţie a dezbaterii publice, indispensabilă oricărei forme de democraţie. Guvernarea poate deveni mai transparentă prin facilitarea accesului la informaţii publice. Forme de scrutin electronic sunt experimentate peste tot în lume. Cu toate acestea, construcţia unei infrastructuri care face comportamentul individual şi interacţiunile de grup perfect vizibile este de natură să afecteze structural democraţia. Acest lucru se întâmplă în primul rând prin modificarea

comportamentului individual, prin internalizarea unei autocenzuri care subminează participarea şi contestarea. În al doilea rând, se întâmplă prin penetrarea grupurilor active din societate şi prin creşterea capacităţii de intervenţie asupra lor. Nu în ultimul rând, prin dezechilibrarea serioasă a raporturilor de putere dintre cei aleşi democratic şi cei care nu au fost aleşi. Infrastructura de supraveghere nu este controlată efectiv de niciun oficial ales, fapt valabil inclusiv în democraţii solide precum Suedia sau Franţa.

Pentru unii, înregistrarea şi stocarea datelor nu reprezintă o problemă, ei preluând argumentul: „Nu fac nimic ilegal şi în consecinţă nu am de ce să mă tem”. Dar ar trebui să fie conştienţi că, de îndată ce sunt stocate undeva, aceste date pot fi extrase, fără ca ei să mai poată avea niciun control asupra lor. În orice moment, elemente care ţin de viaţa personală pot fi accesate, pentru că eşti ţinta supravegherii guvernamentale. Iar această supraveghere este realizată nu pentru că s-a făcut ceva ilegal, ci pentru că persoana ar putea fi problematică din punct de vedere politic. Experienţele de hărţuire şi intimidare guvernamentală prin care au trecut cei care participă la dialogul din volum sunt edificatoare. Dacă faci parte dintr-un ONG care militează împotriva unor proiecte guvernamentale sau dacă eşti jurnalist de investigaţie, dacă faci parte dintr-un partid politic, de opoziţie sau de la guvernare, dacă participi la proteste sau semnezi petiţii publice, toate acestea te pot aduce în atenţia celor care monitorizează. Există foarte puţine garanţii că acest lucru nu ţi se poate întâmpla şi ţie. Tehnologia de supraveghere, stocarea şi folosirea datelor sunt controlate de funcţionari şi experţi care lucrează într-un regim strict de confidenţialitate şi care raportează unor responsabili

militari ce sunt într-o foarte mică măsură răspunzători în faţa conducătorilor politici aleşi. Astfel, cunoaşterea totală este mai accesibilă regimurilor autoritare decât celor democratice, dar în măsură egală posibilă şi tentantă, căci infrastructura supravegherii îi acordă puterii politice o autonomie faţă de societate căreia cu greu i se poate rezista.

Strategii ale rezistenţei

Având în vedere mobilizarea extraordinară a guvernelor şi marilor corporaţii în direcţia digitalizării şi a supravegherii, se pune problema fundamentală a posibilităţii de a rezista. Rezistenţa este cu atât mai dificilă, cu cât viteza cu care întreaga lume se mută în spaţiul virtual este mai mare. Absenţa din virtual poate însemna izolare, vulnerabilitate şi precaritate. Ştim însă că instituţiile politice se transformă pentru a supravieţui, iar odată cu acestea regimurile juridice. Ştim de asemenea că toate instituţiile politice şi tipurile de guvernare au fost contestate de-a lungul timpului. Dar de data aceasta nu discutăm despre un regim, guvern sau ideologie anume, ci despre un *modus operandi* statal care se generalizează indiferent de forma de organizare politică. În volum se discută pe larg despre strategiile de rezistenţă posibile. Cele două strategii discutate şi comparate explicit sunt folosirea „legilor omului”, adică a instituţiilor politice şi juridice, pentru limitarea supravegherii, respectiv folosirea „legilor fizicii ale informaticii”, adică a tehnologiei de anonimizare şi de criptare a comunicaţiilor. Mai adăugăm o strategie de altfel utilizată şi perfecţionată de Wikileaks, şi anume dezvăluirea activităţilor guvernării prin scurgerea de date relevante către public10. Recentele scurgeri de date de la o companie panameză specializată în operaţiuni financiare arată că nu numai guvernarea este

vulnerabilă, ci şi companiile, mai ales acelea care au făcut din secret şi anonimitate un produs11. Nu în ultimul rând, se discută calea transformării culturale, prin care cetăţenii să fie făcuţi conştienţi de răspândirea supravegherii, să fie educaţi în a folosi instrumente de protejare a datelor private şi în a participa la viaţa virtuală în multiple reţele şi grupuri ce rezistă masificării şi centralizării internetului.

Pot funcţiona mecanismele democratice şi juridice în direcţia protecţiei vieţii personale? Până în acest moment, se pare că prea puţin. Inclusiv în ţările cu regimuri democratice considerate solide, instituţiile reprezentative – parlamentele – au dificultăţi majore în a controla executivele şi în principal ramurile militare şi de informaţii ale acestora. Prin agitarea spectrului războiului şi al feluritelor tipuri de ameninţări, are loc o dezvoltare rapidă a infrastructurii digitale şi de supraveghere, slab înţeleasă în funcţionarea ei efectivă şi foarte slab contestată politic în cadrele electorale şi democratice. Cu toate acestea, cel puţin în spaţiul nord-atlantic, au existat victorii importante care arată că presiunea mediatică, publică şi civică poate da rezultate. În Statele Unite, preşedintele Bill Clinton s-a opus operaţionalizării de către Pentagon a două sisteme paralele – Total Information Awareness (TIA) şi The Mother of All Data Bases (Mama tuturor bazelor de date) –, un refuz ce pare a reflecta mai mult o luptă politică internă în care NSA a reuşit să oprească două proiecte pe care nu le controla, şi mai puţin un efect al presiunii publice12. Lupta juridică poate de asemenea să funcţioneze. În 2015, pe 6 octombrie, Curtea Europeană de Justiţie a invalidat acordul dintre Statele Unite şi Uniunea Europeană numit „Safe Harbour”, acord prin care se permitea marilor corporaţii americane să transfere şi să stocheze în Statele Unite datele personale ale cetăţenilor europeni13. Această

invalidare se datorează unui tânăr austriac, Maximillian Schrems, care a făcut o plângere împotriva autorităţilor naţionale irlandeze, care permiteau transferul de date de pe serverele aflate în Irlanda către cele aflate în Statele Unite, unde nu beneficiau de o protecţie suficientă, în volum se discută şi despre lobby-ul eficient realizat de către autorii *Cypherpunks* în faţa Parlamentului European, lobby care împreună cu presiunea publică de pe tot continentul au dus la suspendarea acordului ACTA14. În Europa, curţile constituţionale se află deseori în prima linie de apărare a libertăţilor individuale şi a datelor personale. Reţele de ONG-uri şi de activişti sunt permanent mobilizate pentru a opri tentativele guvernelor şi corporaţiilor de a extinde monitorizarea, conform principiului „anonimitate pentru cei slabi, transparenţă pentru cei puternici”.

A doua strategie, cea a utilizării „legilor fizicii”, este una preponderent tehnică. Aşa cum guvernele şi corporaţiile se află într-o permanentă „cursă a înarmărilor” în privinţa capacităţilor de supraveghere, în mod similar cetăţenii şi societatea civilă trebuie să se angreneze într-o cursă de dezvoltare a capacităţilor de criptare care să o anuleze pe prima. Generalizarea soluţiilor de criptare pare o soluţie ideală, ce va permite în acelaşi timp utilizarea internetului şi o oarecare protecţie, niciodată completă, a datelor personale. Criptarea ajută în depăşirea inconvenientului de a nu fi proprietar *de facto* al nici uneia dintre părţi fizice ale internetului – dispozitive, cabluri, centre de date. Eficienţa acestei metode este probată, paradoxal, tot de către guverne şi corporaţii în cursa pentru securitate şi supremaţie. Guvernele şi-au perfecţionat metodele de criptare pentru a nu fi vulnerabile în faţa adversarilor. De ce nu ar folosi şi

cetăţenii aceleaşi instrumente pentru a se proteja de guverne? 15 Folosirea soluţiilor de criptare nu va elibera internetul, ci va duce la o împărţire a acestuia, având de-o parte giganţii privaţi conectaţi cu guvernele şi de cealaltă o mulţime de comunităţi şi de reţele autonome care îşi construiesc spaţii libere de interacţiune. Aceste reţele şi grupuri nu sunt doar culturale sau economice, ele au o semnificaţie profund politică, căci participă la o reconstrucţie a democraţiei, una de la bază, orizontală şi autonomă, ca alternativă la democraţia formală, centralizată politic şi tehnologic, în care libertatea este compromisă odată cu distrugerea sferei private.16 Aceste spaţii le vor fi însă accesibile numai celor care reuşesc să stăpânească tehnologia. Astfel, o parte din elita high-tech se va transforma şi în avangardă a luptei democratice, o nouă disidenţă care se va opune unei „structuri extrem de restrictive, omogenizate, postmoderne, transnaţionale şi totalitare de o complexitate de necrezut, absurdă şi devalorizată” (Julian Assange).

Care va fi soarta încercărilor de a creşte transparenţa activităţii guvernelor, atât în ceea ce priveşte politica externă şi purtarea războaielor, cât şi în ce priveşte activitatea de supraveghere? Ele probabil vor continua, inspirate de Wikileaks sau de exemplul lui Edward Snowden. Edward Snowden, fost angajat al unei companii private care subcontracta servicii de la Agenţia americană Naţională de Securitate, a fost printre primii care au dezvăluit, cu informaţii din interior, existenţa uriaşului complex de supraveghere pe care îl întreţin SUA şi aliaţii săi occidentali. Virulenţa atacurilor asupra lui Snowden se explică prin faptul că pune guvernarea într-o situaţie delicată, imposibil de legitimat din punct de vedere democratic. Dezvăluirile lui Snowden transformă

ceea ce părea o sursă de putere într-o sursă de vulnerabilitate. Existenţa unui instrument ideal de supraveghere şi control devine o vulnerabilitate majoră, de data aceasta de tip politic şi democratic. Cum mai pot avea încredere cetăţenii, oricât de dispuşi ar fi, într-un guvern care îi spionează permanent? Spectrul terorismului şi al criminalităţii cibernetice pare să nu fie de ajuns pentru a justifica o intruziune de o asemenea magnitudine în viaţa privată a acestora. Ceea ce au aflat guvernele odată cu dezvăluirile mediatizate global ale Wikileaks-ului şi ale lui Snowden este că la rândul lor pot fi monitorizate şi supravegheate, că la rândul lor, ca şi cetăţenii, produc date şi lasă urme digitale. Şi că, în principiu, pot fi trase la răspundere pentru asta.

România. De la totalitarismul ideologic la totalitarismul digital

Unde se află România pe această hartă globală a informaţiei şi supravegherii? Istoria ei recentă, echilibrul precar dintre instituţii şi chiar poziţia geografică o transformă, din păcate, într-o candidată ideală pentru accesul în distopia controlului social. Într-o perioadă foarte scurtă a făcut tranziţia de la totalitarismul ideologic comunist la totalitarismul digital, preluând atât moştenirea supravegherii comuniste, cât şi tendinţele globale ale supravegherii dezvoltate după Războiul Rece. Ceea ce a facilitat acest proces este slăbirea instituţiilor reprezentativ-democratice, care au reuşit doar într-o mică măsură să se impună în faţa executivului şi în special a serviciilor de informaţii. Digitalul şi online-ul sunt terenurile în care democraţia românească îşi testează viabilitatea şi forţa. Pentru moment, ceea ce ar fi trebuit să facă partidele şi Parlamentul, şi anume a apăra drepturile fundamentale şi viaţa privată, este *de facto* delegat

societăţii civile, presei şi instituţiilor care încă rezistă presiunilor, de exemplu Curtea Constituţională.

În anul 1989 România era o ţară izolată, condusă cu o mână de fier de un cuplu prezidenţial, o elită de partid şi un aparat poliţienesc masiv, Securitatea. După ce se îndepărtase atât de Uniunea Sovietică, cât şi de ţările occidentale, regimul politic avea toate motivele să creadă că se afla în pericol. Baza socială se clătina, aşa cum arătase Braşovul în 1987, tehnocraţia economică nu mai dădea rezultate, iar birocraţia de partid obosise. În aceste condiţii, supravieţuirea regimului depindea de succesul intimidării şi al represiunii, care la rândul lor depindeau de abilitatea Securităţii de a urmări cetăţenii. Practicile de violare a corespondenţei, ascultare ambientală şi ascultare a telefoanelor se banalizaseră. Cenzura oficială era dublată de o eficientă autocenzură a comportamentului individual. În cele din urmă, operaţiunea masivă de interceptare şi ascultare a dat greş, lanţul evenimentelor din decembrie 1989 petrecându-se prea rapid pentru ca supravegherea să mai conteze. După căderea comunismului, procesul de lustraţie nu a demarat convingător, iar aparatul de partid şi cel de Securitate şi-au continuat existenţa în noile cadre democratice. Au urmat nişte ani tensionaţi şi confuzi în care practicile de supraveghere masivă au fost limitate, deşi nu a fost clar dacă tehnica şi personalul au dispărut.

Integrarea euroatlantică, scop declarat al României în tranziţia sa timpurie, a presupus şi reforma sectorului militar şi de informaţii. Ideea controlului civil asupra acestora era o condiţionalitate a NATO, iar această condiţionalitate a impulsionat procesul de reformă pentru care presiunile publică şi politică interne erau prea slabe. Armata a trecut printr-un proces mai transparent de reformă, care a presupus atât eliminarea serviciului militar

obligatoriu, cât şi reducerea semnificativă a personalului şi capacităţilor de luptă. Reforma serviciilor de informaţii, în mod expres cerută de partenerii nord-atlantici, a fost mult mai discretă şi lipsită de vigoare, dar cu un impact mare asupra politicii şi a economiei. Dacă relaţiile elitei civile cu Armata nu fuseseră problematice nici măcar în comunism, cele cu serviciile secrete erau mai complicate. În timp se construiseră nişte instituţii mult mai puternice şi mult mai autonome decât cele ale Armatei. Iar pericolul pentru tânăra democraţie românească era mult mai mare. Reforma serviciilor a presupus pensionarea sau ieşirea din sistem a unui număr important de foşti angajaţi. Mulţi au intrat în afaceri, construind o zonă gri, în care se acţionează prin aparenta respectarea a legilor pieţei, dar în care se păstrează legături puternice cu instituţiile pe care. În principiu aceştia le-au părăsit. Poate nu întâmplător, unele dintre ramurile economice cel mai serios penetrate de aceste grupări au fost cele de telecomunicaţii şi IT. În paralel s-a continuat reconfigurarea rolului instituţional al serviciilor secrete. Schimbarea majoră a intervenit în 2004, odată cu alegerea unui nou preşedinte. Şocul atentatelor de la New York a produs nu doar teamă, ci şi o reconfigurare a ţintelor şi metodelor de lucru. Lupta antiteroristă, configurată pe modelul american, a început să fie exportată peste tot în lume. Această luptă, aşa cum am arătat anterior, întăreşte şi mai mult statul în raport cu cetăţenii, în special în ceea ce priveşte supravegherea. România, deja parte a NATO, deşi nu avea o problemă teroristă pe teritoriul ţării, a transferat şi adaptat modelul. Pentru serviciile secrete din România, dar nu numai, acest lucru a fost o gură de aer proaspăt, fiindu-le astfel reconfigurate rolul şi legitimitatea. În noul cadru, acestea nu mai reprezintă

instituţiile care au ajutat regimul comunist, ci o parte importantă a luptei globale împotriva terorismului, deci pentru libertate şi democraţie.

În al doilea rând, şi acest lucru este valabil în special pentru serviciile secrete româneşti, ele au fost instrumentalizate în lupta anticorupţie, identificată drept ameninţare la adresa securităţii naţionale. Acest diagnostic e acceptat şi susţinut de o mare parte a opiniei publice. Comparativ cu lupta antiteroristă, cea anticorupţie are un mare avantaj din perspectiva creşterii influenţei serviciilor şi a generalizării supravegherii. Dacă „teroristul" este pentru cetăţeni o prezenţă rară, exotică şi neclară, „coruptul" este o prezenţă familiară şi răspândită în toate straturile societăţii. Un „duşman" intern ideal, a cărui urmărire presupune accesul oriunde, de la instituţii publice şi până la tribunale, spitale şi şcoli. Cele două justificări ale supravegherii au mers în paralel, punctate permanent în spaţiul public de către reprezentanţii formali şi informali ai serviciilor secrete. Războiul civil din Siria, izbucnirea unui scurt război civil în Ucraina, criza refugiaţilor, atentatele din noiembrie 2015 din Franţa şi cele din aprilie 2016 din Belgia, toate au fost folosite pentru a sublinia nevoia de stabilitate şi securitate, naraţiunea principală a instituţiilor de forţă.

În această configuraţie în care instituţiile democratice par că au pierdut controlul asupra serviciilor de informaţii, cât de răspândită este supravegherea? 17 Este extinsă şi se va extinde în continuare. Ca orice al cetăţean al lumii care foloseşte serviciile unor giganţi ai internetului şi tehnologiei, cetăţeanul român are datele reţinute şi stocate undeva. Nu este foarte clar ce date şi informaţii sunt puse la dispoziţia serviciilor din România, atât de către marile companii, cât şi de către guvernul

american. Într-o anumită măsură, nici nu contează, atât timp cât aceste instituţii sunt conectate direct la serverele providerilor de servicii de internet şi de comunicaţii mobile. Instituţia care gestionează activitatea de interceptare este SRI, prin Centrul Naţional de Interceptare a Comunicaţiilor (CNIC), iar entitatea respectivă a acţionat într-un vid legislativ în care nu era clar ce responsabilităţi şi puteri are, în special în ceea ce priveşte protejarea drepturilor fundamentale şi a datelor cu caracter personal. Vidul legislativ nu l-a împiedicat însă să opereze. Cifrele arată o creştere semnificativă de la an la an a mandatelor de interceptare18.

În luna martie 2016 însă, Curtea Constituţională a decis că interceptările realizate de către SRI nu pot fi acceptabile ca probe în instanţă. Această decizie a transmis o undă de şoc, pentru că majoritatea dosarelor de corupţie au fost instrumentate cu ajutorul tehnicii de interceptare a SRI, instituţie ce are o situaţie de cvasimonopol asupra interceptărilor. Repoziţionarea instituţiilor a fost rapidă. Consiliul Suprem de Apărare a Ţării, un adevărat guvern paralel gestionat de către preşedinţie, a propus schimbarea legislaţiei prin ordonanţă de urgenţă şi astfel SRI a devenit organ special de cercetare penală, cu dreptul de a participa la instrumentarea dosarelor care ţin de siguranţa naţională şi terorism. Soluţia găsită a fost criticată de societatea civilă ca fiind foarte probabil neconstituţională 19. Mai mult, conform strategiei privind siguranţa naţională, aceasta este definită foarte extins20. Astfel, există puţine garanţii instituţionale şi procedurale că temeiul siguranţei naţionale va fi invocat corect şi proporţional. Prin aceeaşi ordonanţă de urgenţă, CNIC este obligat să asiste organele de urmărire penală atunci când au un mandat de

supraveghere tehnică dispus de instanţele de judecată conform dispoziţiilor Codului de procedură penală. Persistă însă neclarităţile de ordin legal şi constituţional, precum şi garanţiile că datele personale sunt protejate conform principiilor Cartei drepturilor fundamentale a Uniunii Europene21.

După atentatele din luna martie 2016 de la Bruxelles, în mod previzibil, s-a solicitat de către guvern şi preşedinţie rediscutarea şi aprobarea în regim de urgenţă a aşa-numitului pachet „Big Brother", ce cuprinde prevederi privind siguranţa cibernetică a României. De asemenea, prin declaraţii publice ale reprezentanţilor executivului şi ai serviciilor de informaţii s-a încercat în mod neconvingător să se lege atentatele teroriste şi conflictele din Orientul Mijlociu de folosirea cartelelor prepay din România, care în prezent pot fi cumpărate fără a fi nevoie de identificarea cumpărătorului. Obligativitatea declarării identităţii este un alt obiectiv asumat de către serviciile de informaţii. Pachetul iniţial „Big Brother" a fost analizat de Curtea Constituţională şi declarat neconstituţional (Decizia Curţii Constituţionale nr. 17/2015). Societatea civilă a solicitat în mai multe rânduri dezbateri pe tema pachetului, a venit cu propuneri de amendare, dar acestea nu s-au concretizat22. Astfel, pare că s-a ajuns la un blocaj în care executivul, inclusiv preşedinţia, invocă pericolul terorist, dar refuză dialogul cu societatea civilă şi nu pare capabil să prezinte propuneri viabile din punct de vedere constituţional.

Instalarea Leviatanului digital în România este întâmpinată cu rezistenţă, în principal din partea societăţii civile, a opiniei publice, a unei mici părţi a presei şi a sectorului privat de comunicaţii şi, foarte important, din partea Curţii Constituţionale. Ceea ce însă este oprit sau

amânat ca demers legislativ se petrece deja în realitate. Comunicaţiile unui număr foarte mare de cetăţeni sunt supravegheate şi stocate. Este posibil ca aceste comunicaţii să nu poată fi folosite în instanţă, dar de cele mai multe ori nici nu este nevoie. Acestea se pot scurge către presă, aşa cum s-a mai întâmplat, sau pot fi folosite ca instrumente de presiune şi şantaj. Contextul internaţional nu este favorabil protecţiei vieţii private şi a comunicaţiilor, şi ţara noastră nu se poate extrage acestuia. Iar acest context este folosit pentru a extinde supravegherea, împărţită între diferite agenţii guvernamentale străine şi naţionale, mari corporaţii şi companii care oferă soluţii de supraveghere. Mai devreme sau mai târziu, în paralel cu rezistenţa civică şi politică împotriva legalizării acesteia, e posibil să fie nevoie să ne alfabetizăm cu toţii în folosirea sigură a internetului şi a programelor. Dar numai dacă preţuim libertatea şi protecţia sferei private, două lucruri care au lipsit acestei societăţi înainte de 1989 şi de care ar fi trebuit să ne bucurăm odată cu tranziţia la democraţie.

Claudiu Crăciun

1. FBI-ul american a anunţat recent că a reuşit să intre în telefonul Apple al unei persoane implicate într-un atac terorist fără ajutorul companiei, după ce aceasta a refuzat să asiste autorităţile. Accesarea datelor a fost posibilă cu ajutorul unei firme private.

2. Influenţa guvernamentală americană asupra politicii internetului pare să se diminueze, trecându-se către o guvernanţi internaţională. ICANN, organismul care stabileşte regulile de atribuire de nume de domenii Internet şi de adrese IP, este supravegheat de un Comitet Consultativ Guvernamental din care fac parte toate statele lumii. Este notabilă şi dezvoltarea Forumului Guvernanţei

Internetului, susţinut de Organizaţia Naţiunilor Unite.

3. Dezvăluirile lui Edward Snowden arată cât de extinsă este activitatea de supraveghere, acesta referindu-se şi la convorbirile telefonice şi mesajele text, nu exclusiv la internet. Monitorizarea ţinteşte nu numai cetăţenii ci şi lideri politici de peste tot din lume, inclusiv din ţările NATO, aliate ale SUA; vezi Glenn Greenwald (2015), *No Place to Hide*: *Edward Snowden, the NS A, and the US. Surveillance State*, Picador, şi www.glenngreenwald.net.

4. Pentru o analiză mai detaliată, vezi Julian Assange (2014), *When Google Met Wikileaks*, OR Books

5. Vezi James C. Scott (2007), în numele statului. Modele eşuate de îmbunătăţire a condiţiei umane, Polirom

6. Vezi Michel Foucault (2005), *A supraveghea şi a pedepsi*. Editura Paralela 45

7. Cei patru cavaleri ai Infoapocalipsei, cei pe care guvernele îi invocă pentru a extinde supravegherea, sunt, conform lui Julian Assange: terorismul, pornografia infantilă, spălarea banilor şi traficul de droguri.

8. De exemplu, guvernul german a fost autorizat să instaleze programe de tip troian pentru accesarea comunicaţiilor persoanelor suspecte; *German government to use Trojan spyware to monitor citizens*, Deustehe Welle, 22.02.2016: http://www.dw.com/en/ german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629 (accesat în data de 4 aprilie 2016).

9. *Jlntemet est devenit le système nerveux de nos sociétés** interviu luat de către Alexandre Lacroix lui Julian Assange, *Philosophie Magazine*, 30.05.2013: http://www.phik>mag.com/lépoque/reportage/julian-assange-intemet-est-devenu-le-systeme-nerveux-de-nos-societes-7525 (accesat în data de 4 aprilie 2016)

10. *Ce este Wikileaks*, 3.11.2015:

https://wikileaks.org/What-is-Wikileaks.html (accesat în data de 4 aprilie 2016)

11. *Panamá Papers*: *The secrets of dirty money*, Süddeutsche Zeitung: http://panamapapers.sueddeutsche.de/en/ (accesat în data de 4 aprilie 2016)

12. Vezi dialogul lui Julian Assange eu Ignacio Ramonet în Ignacio Ramonet (2015), *L'Empire de la surveillance*, Galilee, pp. 147 – 149

13. Curtea de Justiţie a Uniunii Europene, Luxemburg, 6.10.2015, Decizia C-362/14, Maximillian Schrems v Data Protection Commissionen http://curia.Europa.eu/ jems/upload/docs/application/pdf/2015 – 10/cpl50117 en.pdf (accesat în data de 4 aprilie 2016)

14. Campania a fost coordonată de organizaţia franceză La Quadrature du net. Mai multe informaţii despre campanie se pot găsi aici http://www.laquadrature.net/en/acta (accesat în data de 4 aprilie 2016).

15. O variantă interesantă este supravegherea de „jos în sus" de către cetăţeni a autorităţilor (*sousveillance*) *y* vezi David Bollier, *Sousveillance as a Response to Surveillance*, 24.11.2013: http://bollier.org/blog/sousveillance-response-surveillance (accesat în data de 4 aprilie 2016).

16. Eric Hughes (1993), *A Cypherpunk's Manifeste* –, http://www.activism.net/cypherpunk/manifesto.html (accesat în data de 4 aprilie 2016)

17. Conform estimărilor, personalul de 12.000 de agenţi secreţi e depăşit doar de al FBI. Cu o populaţie de 2, 5% din totalul grupului de ţări, România are mai mult de 15% din agenţii grupului; în ceea ce priveşte proporţia faţă de populaţie: există 60 de angajaţi în serviciile interne la suta de mii de locuitori. Următorul clasat, Polonia, are 13

angajaţi; bugetul SRI are cea mai mare pondere în cheltuielile publice: jumătate de procent, de cinci ori mai mult decât media celor 10 state, care este de o zecime de procent. FBI se descurcă cu doar o şeptime de procent din cheltuielile publice totale ale SUA. Şi, în termeni absoluţi, SRI reuşeşte să cheltuiască mai mult decât serviciile omoloage din Germania, Franţa, Italia sau Polonia. Estimările au fost realizate de Lucian Davidescu, *Cât de mare este SRI – faţă de serviciile din alte ţări*, *14.09.2014*: http://riscograma.ro/9129/cat-de-mare-este-sri-fata-de-serviciile-din-alte-tari/ (accesat în data de 4 aprilie 2016).

18. Din datele Rapoartelor anuale ale SRI se desprind următoarele cifre: 2005 – 6 370 de mandate, 2006 – 8 693 de mandate, 2007 – 10 272 de mandate, 2008 – 15 170 de mandate, 2009 – 22 176 de mandate; 2010 – 30 624 de mandate, 201135 678 de mandate, 2012 – 36 085 de mandate, 2013 – 38 884 de mandate, Radu Tudor, *Interceptări*: *600% creştere în ultimii 10 anii* 27.01.2015: http://radu-tuclor.ro/interceptări-600-cresterc-in-ultimii-10-ani/ (accesat în data de 4 aprilie 2016).

19. *Metodele speciale de supraveghere*. *Societatea civilă cere garanţii legale privind respectarea drepturilor omului*, TVR, 31.03.2016: http://ştiri.tvr.ro/metodelespeciale-de-supraveghere-societatea-civila-cere-garantii-legle-privind-respectareadrepturilor-omului 72601.html (accesat în data de 6 aprilie 2016).

20. „Strategia reflecta necesitatea promovării unui concept de securitate naţională extinsă – fundamentat pe democraţia constituţională şi respectul mutual dintre cetăţeni şi stat – care vizează interesele care converg spre asigurarea securităţii naţionale, manifestate în următoarele domenii: apărare (înţeleasă în dublă calitate normativă, de apărare naţională şi apărare colectivă),

ordine publică, activitatea de informaţii, contrainformaţii şi de securitate, educaţie, sănătate, economic, energetic, financiar, mediu, infrastructuri critice”, Strategia Naţională de Apărare a Ţării: http://www.presidency.ro/files/userfiles/Strategia Naţionala de Apărare a Ţării 1.pdf (accesat în data de 6 aprilie 2016).

21. Carta drepturilor fundamentale a Uniunii Europene, Articolul 8. Protecţia datelor cu caracter personal: (1) Orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc. (2) Asemenea date trebuie tratate în mod corect, în scopurile precizate şi pe baza consimţământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum şi dreptul de a obţine rectificarea acestora. (3) Respectarea acestor norme se supune controlului unei autorităţi independente. http://eur-lex. Europa.eu/legal-content/RO/TXT /? un = CELEX%3 A12012P%2FTXT (accesat în data de 6 aprilie 2016).

22. Vezi documentul Asociaţiei pentru Tehnologie şi Internet, susţinut de alte şase ONG-uri, *Comentarii la propunerea de lege privind securitatea cibernetică*, APŢI, 25.02.2015: https://www.apţi.rb/comentarii-proiect-lege-securitate-cibernetca2016 (accesat în data de 2 aprilie 2016).

Ce este un *cypherpunk*?

Activiştii *cypherpunk* militează pentru folosirea criptografiei şi a unor metode similare ei pentru a efectua schimbări de natură socială sau politică.1 Fondată la începutul anilor ’90, această mişcare a avut activitatea cea mai intensă în perioada „războaielor criptografice” din anii ’90 şi în urma „primăverii internetului” din 2011. Termenul de *cypherpunk*, derivat din (criptograficul) *cipher* şi *punk*,

a fost introdus în Oxford English Dictionary în 2006.2

Introducere:

O chemare sub armele criptografice

Această carte nu este un manifest. Nu mai este timp pentru aşa ceva. Această carte este un avertisment.

Lumea nu alunecă pe nesimţite către o nouă distopie transnaţională, ci se îndreaptă spre ea cu paşi repezi. Acest fenomen nu a fost suficient recunoscut în afara cercurilor de securitate naţională. A fost ţinut ascuns prin tăinuire, complexitate şi dimensiune. Internetul, cel mai valoros instrument de emancipare al nostru, a fost transformat în cel mai periculos mijlocitor al totalitarismului care a fost văzut vreodată. Internetul e o ameninţare la adresa viitorului civilizaţiei umane.

Aceste transformări au survenit pe tăcute, din cauză că cei care ştiu ce se întâmplă lucrează în industria supravegherii globale şi nu au niciun motiv să vorbească deschis. Dacă e lăsată să continue pe această cale, civilizaţia globală va deveni în câţiva ani o distopie postmodernă a supravegherii, din care scăparea nu va fi posibilă decât pentru cei mai pricepuţi dintre noi. De fapt, s-ar putea să se fi ajuns deja acolo.

Deşi mulţi scriitori au în vedere semnificaţia internetului pentru civilizaţia globală, ei se înşală. Se înşală pentru că nu au acel simţ al perspectivei pe care-l oferă experienţa directă. Se înşală pentru că nu s-au întâlnit niciodată cu inamicul.

Nicio descriere a lumii nu supravieţuieşte primului contact cu inamicul.

Noi am întâlnit inamicul.

În ultimii şase ani [până la editarea acestui volum – 2012], Wikileaks a intrat în conflict cu aproape fiecare stat puternic. Cunoaştem noul regim de supraveghere din

interior, pentru că i-am aflat secretele. îl cunoaştem dintr-o perspectivă a combatantului, pentru că a trebuit să ne protejăm oamenii, resursele financiare şi informatorii. îl cunoaştem dintr-o perspectivă globală, pentru că avem oameni, active şi informaţii în aproape fiecare ţară din lume. îl cunoaştem dintr-o perspectivă temporală, pentru că luptăm împotriva acestui fenomen de ani de zile şi l-am văzut dublându-se şi răspândindu-se, iar şi iar. Este un parazit cotropitor, ce se hrăneşte cu societăţile care se conectează la internet. Se întinde pe întreaga planetă, infectând fiecare stat şi popor în calea sa.

Ce este de făcut?

Odată ca niciodată, într-un loc care nu e nici aici, nici acolo, noi, creatorii şi cetăţenii tânărului internet, am discutat despre viitorul noii noastre lumi.

Am văzut că relaţiile dintre oameni vor fi mediate de noua noastră lume şi că natura statelor, care se definesc prin felul în care oamenii schimbă informaţii, valoare economică şi forţă, se va schimba şi ea.

Am văzut că fuziunea dintre structurile statale existente şi internet a creat posibilitatea schimbării naturii statelor.

În primul rând, amintiţi-vă că statele sunt acele sisteme prin care curge forţa coercitivă. Facţiunile din cadrul unui stat pot concura pentru susţinere, lucru care duce la fenomene democratice de suprafaţă, dar la temelia statelor stau aplicarea, respectiv evitarea sistematică a violenţei. Proprietatea asupra pământului, proprietăţile, chiriile, dividendele, taxele, amenzile judiciare, cenzura, drepturile de autor şi mărcile comerciale sunt impuse prin ameninţarea cu aplicarea violenţei statale.

De cele mai multe ori nici nu suntem conştienţi de cât de aproape suntem de violenţă, pentru că facem cu

toţii concesii pentru a o evita. Asemenea marinarilor care adulmecă briza mării, rareori ne oprim să reflectăm la întunericul pe care se sprijină lumea noastră de la suprafaţă.

Care va fi mijlocitorul forţei coercitive în noul spaţiu al internetului?

Are vreun sens să ne punem întrebarea aceasta? Există vreun loc pentru noţiunea de violenţă coercitivă în acest spaţiu imaterial, acest tărâm platonic al ideilor şi al fluxului de informaţii? O forţă care poate să modifice arhivele istorice, să asculte telefoanele, să dezbine popoarele, să transforme complexitatea în dărâmături şi să ridice ziduri, asemenea unui armate de ocupaţie?

Natura platonică a internetului, a fluxului de idei şi informaţii, este coruptă de originile sale fizice. Bazele sale sunt cablurile cu fibră optică ce se desfăşoară pe fundul oceanelor, sateliţii care se învârt deasupra capetelor noastre, serverele adăpostite în clădirile din oraşe ce se întind de la New York la Nairobi. Asemenea soldatului care l-a ucis pe Arhimede cu o simplă sabie, se poate întâmpla ca o miliţie bine înarmată să pună mâna pe vârful dezvoltării civilizaţiei occidentale, tărâmul nostru platonic.

Noua lume a internetului, separată de vechea lume a atomilor bruţi, tânjea după independenţă. Dar statele şi aliaţii lor şi-au propus să controleze noua noastră lume – prin controlul substratului său fizic. Statul, asemenea unei armate în jurul unui puţ de petrol sau unui agent vamal care caută să smulgă mită la frontieră, va învăţa în scurt timp să se folosească de controlul pe care-l deţine asupra spaţiului fizic pentru a ajunge să controleze tărâmul nostru platonic. Va împiedica independenţa la care am visat pentru ca apoi, ghemuit lângă cablurile optice şi în jurul staţiilor de recepţie la sol a informaţiilor de la sateliţi, să

înceapă să intercepteze în masă fluxul de informaţii al noii noastre lumi – însăşi esenţa sa – exact atunci când fiecare relaţie umană, economică sau politică va fi aderat la acesta. Statul se va infiltra în venele şi arterele noilor noastre societăţi, înhăţând fiecare relaţie exprimată sau comunicată, fiecare pagină web citită, fiecare mesaj trimis şi fiecare cuvânt căutat pe Google, iar apoi va stoca pentru totdeauna toate aceste lucruri ştiute de ea, miliarde de interceptări zilnice, o putere nemaivăzută, în uriaşe depozite secrete. Va extrage fără încetare din această comoară, producţia intelectuală privată a întregii omeniri, cu algoritmi de căutare sau de recunoaştere după tipar din ce în ce mai sofisticaţi, îmbogăţind comoara şi mărind la maximum discrepanţa de putere dintre cei interceptaţi şi cei care interceptează. Iar apoi, statul va folosi în lumea fizică ceea ce a aflat, pentru a declara războaie, pentru a dirija atacuri cu dronă, pentru a manipula comisiile ONU şi tratatele comerciale şi pentru a-şi favoriza propria şi vasta reţea de industrii, de prieteni şi de persoane care cunosc dedesubturile.

Dar noi am descoperit ceva. Singura noastră speranţă împotriva dominaţiei totale. O speranţă pe care, cu curaj, discernământ şi solidaritate o vom putea folosi pentru a opune rezistenţă. O proprietate stranie a universului fizic în care trăim.

Universul crede în codare.

Este mai uşor să codezi o informaţie decât să o decodezi.

Am observat că putem folosi această stranie proprietate pentru a crea legile unei lumi noi. Pentru a separa noul nostru tărâm platonic de temeliile sale fizice, de sateliţi, de cabluri oceanice şi de cei care le controlează. Pentru a ne fortifica spaţiul în spatele unei

cortine criptografice. Pentru a crea tărâmuri noi, la care cei care controlează realitatea fizică nu au acces, fiindcă ar avea nevoie de resurse infinite ca să ne urmeze pe acele căi.

Şi, astfel, pentru a ne declara independenţa.

Savanţii din Proiectul Manhattan au descoperit că universul permite construcţia bombei atomice. Aceasta nu era o concluzie evidentă. S-ar fi putut ca armele nucleare să nu se supună legilor fizice. Totuşi, universul crede în bombe atomice şi reactoare nucleare. Ele sunt un fenomen pe care universul îl binecuvântează, asemenea sării, mării sau stelelor.

La fel, universul, universul nostru fizic, are acea proprietate care face posibil ca un individ, sau un grup de indivizi, să cifreze un lucru într-un mod sigur, automat, chiar şi fără să ştie, în aşa fel încât toate resursele şi toată voinţa politică a celei mai mari superputeri din lume să nu-l poată descifra. Iar căile pe care cifrarea le formează între oameni se pot uni pentru a crea regiuni întregi eliberate de forţa coercitivă a statului exterior. Eliberate de interceptarea în masă. Eliberate de controlul statal.

În acest fel, oamenii îşi vor putea opune propria voinţă voinţei unei superputeri mobilizate şi vor putea învinge. Criptarea este o întruchipare a legilor fizicii, iar ea nu ascultă de ameninţările gălăgioase ale statelor, fie acestea şi distopii transnaţionale ale supravegherii.

Nu este un lucru evident că lumea trebuia să funcţioneze în acest fel. Dar cumva universul priveşte criptarea cu bunăvoinţă.

Criptografia este forma supremă a acţiunii nonviolente directe.

Deşi statele care deţin armament nuclear pot exercita o violenţă nelimitată chiar asupra a milioane de

oameni, criptografia puternică face ca un stat, chiar folosindu-se de o violenţă nelimitată, să nu poată viola intenţia indivizilor de a ţine secrete faţă de el.

Criptografia puternică poate rezista unui uz nelimitat al violenţei. O problemă de matematică nu va putea fi rezolvată niciodată prin forţă coercitivă.

Dar am putea oare să luăm acest fenomen straniu al lumii noastre şi să-l transformăm într-unul dintre blocurile fundamentale, emancipatoare cu care să construim independenţa omenirii în tărâmul platonic al internetului? Iar pe măsură ce societăţile se vor fi conectat la internet, vom putea reflecta acea libertate înapoi în realitatea fizică pentru a redefini statul?

Amintiţi-vă că statele sunt sistemele care determină unde şi cum se va aplica de regulă forţa coercitivă.

Răspunsul la întrebarea câtă forţă coercitivă din lumea fizică se poate infiltra în tărâmul platonic al internetului este dat de criptografie şi de idealurile cypherpunk.

Pe măsură ce statele se conectează la internet şi viitorul civilizaţiei noastre devine una cu viitorul internetului, trebuie să redefinim relaţiile de forţă.

Dacă nu facem acest lucru, universalitatea internetului va transforma omenirea globală într-o reţea uriaşă de supraveghere şi control în masă.

Trebuie să dăm alarma. Această carte este strigătul în noapte al unui străjer.

În data de 20 martie 2012, aflându-mă în arest la domiciliu în Regatul Unit şi aşteptându-mi extrădarea, m-am întâlnit cu trei prieteni şi camarazi de strajă cu gândul că, poate, vocile noastre la unison i-ar putea trezi pe locuitorii cetăţii. Trebuie să împărtăşim ceea ce am aflat cât încă mai este o şansă ca tu, cititorule, să înţelegi şi să

reacţionezi la ce se întâmplă.

A venit timpul să luăm în mână armele noii noastre lumi, să luptăm pentru noi înşine şi pentru cei pe care-i iubim.

Sarcina noastră este să asigurăm autodeterminarea unde încă se mai poate, să oprim înaintarea distopiei acolo unde nu se mai poate, iar dacă orice altceva va eşua, să-i accelerăm autodistrugerea.

Julian Assange, Londra, octombrie 2012

Participanţii la discuţie

JULIAN ASSANGE este redactorul-şef şi vizionarul din spatele Wikileaks.3 Iniţial un colaborator la lista de e-mailuri Cypherpunk, Julian este astăzi unul dintre exponenţii cei mai proeminenţi ai filosofiei cypherpunk din lume. Activitatea sa în cadrul Wikileaks a conferit popularitate politică expresiei tradiţionale a mişcării cypherpunk: „Confidenţialitate pentru cei slabi, transparenţă pentru cei puternici". În timp ce activitatea sa cea mai vizibilă presupune un exerciţiu viguros al libertăţii de exprimare pentru a constrânge instituţiile puternice la transparenţă şi pentru a le trage la răspundere, el este de asemenea un critic acerb al încălcării abuzive a confidenţialităţii individuale de către stat şi corporaţii. Julian este autorul a numeroase proiecte de software inspirate de filosofia cypherpunk, cum ar fi primul *port scanner* strobe. e pentru TCP/IP, sistemul de fişiere Rubberhose pentru cifrare negabilă[2] şi codul original pentru Wikileaks.4 În adolescenţă, Julian a fost unul dintre primii care au făcut cercetări în ceea ce priveşte confidenţialitatea datelor computerelor şi

2 în engleză deniable encryptiony un sistem de criptare ce permite negarea existenţei unui mesaj sau fişier criptat din cauză că nu se poate dovedi existenţa acestuia, (n.tr.)

reţelelor, înainte ca unele tipuri de *hacking* să fie definite prin lege ca activităţi criminale. Devenit apoi activist şi furnizor de internet în Australia în anii ’90, Julian este de asemenea coautorul cărţii *Underground*, scrisă împreună cu Suelette Dreyfus şi care reprezintă o istorie a mişcării internaţionale a hackerilor, carte care a inspirat în mare parte filmul *Underground*: *The Julian Assange Story.5*

JACOB APPELBAUM este unul dintre fondatorii comunităţii

Noisebridge din San Francisco, membru al organizaţiei Chaos

Computer Club din Berlin şi dezvoltator.6 Jacob este un partizan al Proiectului Tor şi cercetător în cadrul acestuia – un sistem care >

garantează confidenţialitatea online şi care permite tuturor oamenilor să se opună supravegherii şi să împiedice cenzura internetului.7 În ultimul deceniu, interesul său a fost să ajute activiştii pentru protecţia mediului şi drepturile omului. În acest sens a publicat cercetări inedite despre securitate, confidenţialitate şi anonimitate într-o mulţime de domenii de cercetare, de la expertiza informatică la marijuana în scop medical. Jacob este de părere că fiecare are dreptul să citească liber, fără restricţii, şi dreptul să se exprime liber, fără excepţii. În anul 2010, când Julian nu a putut ţine o conferinţă în New York, Jacob a ţinut-o în locul său. De atunci el, prietenii săi şi familia sa au fost hărţuiţi de către guvernul Statelor Unite: interogaţi la aeroporturi, supuşi unor percheziţibnări intruzive şi ameninţaţi de către reprezentanţi ai legii cu viitoare agresiuni sexuale în închisoare; i-a fost confiscat echipamentul, iar activitatea online i-a fost supusă unei somaţii secrete. Jacob nu se lasă însă intimidat de aceste măsuri, continuă să lupte în

procesele juridice aflate în desfăşurare şi rămâne un apărător declarat al libertăţii de exprimare şi un susţinător zelos al Wikileaks.

ANDY MULLER-MAGUHN este membru veteran al Chaos Computer Club din Germania, fost membru al consiliului său de conducere şi purtător de cuvânt.8 Este unul dintre cofondatorii EDRI, European Digital Rights, un ONG care militează pentru respectarea drepturilor omului în epoca digitală.9 în perioada 2000 – 2003 a fost ales de către utilizatorii europeni de internet în funcţia de director european al ICANN, *Internet Corporation for Assigned Names and Numbers*, care este responsabilă cu politicile globale de reglementare a modului în care funcţionează „numele şi numerele" de pe internet.10 Este un specialist în supravegherea telecomunicaţiilor şi în alte tipuri de supraveghere şi lucrează, în calitate de jurnalist, în domeniul industriei supravegherii cu proiectul său wiki, buggedplanet.info. H Andy lucrează în domeniul comunicaţiilor criptografice şi a creat împreună cu alţii o companie numită Cryptophone, care vinde dispozitive pentru comunicare vocală confidenţială clienţilor comerciali şi furnizează consultanţă strategică în contextul arhitecturii de reţea.12

JÉRÉMIE ZIMMERMANN este cofondatorul şi purtătorul de cuvânt al organizaţiei La Quadrature du Net, care militează pentru drepturile cetăţeanului, cea mai proeminentă organizaţie europeană pentru apărarea drepturilor la anonimitate online şi pentru aducerea la cunoştinţa pubicului a atacurilor normative împotriva libertăţilor online.13 Jérémie lucrează la construirea de instrumente pe care publicul să le poată folosi pentru a participa la dezbaterile publice şi pentru a încerca să schimbe lucrurile. Este implicat cel mai mult în cadrul

războaielor drepturilor de autor, al dezbaterii despre neutralitatea reţelei şi al altor aspecte normative care sunt esenţiale pentru viitorul unui internet liber. Recent, grupul său, La Quadrature du Net, a repurtat o victorie de importanţă istorică în politica europeană, orchestrând o campanie publică pentru a respinge Acordul Comercial de Combatere a Contrafacerii (ACTA) în Parlamentul European. La scurt timp după ce a participat la conversaţia care stă la baza acestei cărţi, Jérémie a fost oprit de către doi agenţi FBI în timp ce părăsea Statele Unite şi a fost supus unui interogatoriu despre Wikileaks.

Nota editorului

Pentru a creşte accesibilitatea acestei cărţi pentru publicul general, fiecărui participant la discuţia iniţială i s-a acordat posibilitatea de a dezvolta, clarifica şi face adnotări la punctele principale ale argumentaţiei sale. Ordinea generală a manuscrisului editat corespunde dinamicii discuţiei iniţiale.

Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei

În discuţia care urmează se vor face mai multe referiri la evenimente recente din istoria organizaţiei Wikileaks şi a activităţii sale publicistice. Acestea ar putea fi necunoscute unor cititori nefamiliarizaţi cu povestea Wikileaks, aşa că vor fi rezumate aici.

Wikileaks are misiunea de a primi informaţii de la cei care trag semnale de alarmă, de a le face publice, iar apoi de a se apăra împotriva inevitabilelor atacuri juridice şi politice. Este ceva obişnuit ca state şi organizaţii importante să încerce să împiedice apariţia publicaţiilor Wikileaks şi, fiind unul dintre editorii la care se apelează când orice altceva eşuează, Wikileaks a fost conceput să îndure astfel de dificultăţi.

În 2012, Wikileaks a scos cele mai cunoscute publicaţii ale sale până la această dată, dezvăluind abuzul sistematic asociat secretelor de stat în cadrul armatei şi guvernului SUA. Aceste publicaţii sunt cunoscute sub numele de Collateral Murder, The War Logs şi Cablegate.14 Reacţia a fost un efort concertat şi neîntrerupt al guvernului SUA şi al aliaţilor săi de a distruge Wikileaks.

Marele juriu pentru Wikileaks

Ca o consecinţă directă a publicaţiilor Wikileaks, guvernul SUA a lansat o investigaţie penală în cadrul căreia mai multe organizaţii colaborează împotriva lui Julian Assange şi a personalului Wikileaks, precum şi a susţinătorilor şi a presupuşilor asociaţi ai ei. Un Mare Juriu a fost convocat în Alexandra, Virginia, cu susţinerea Departamentului de Justiţie şi a FBI-ului, pentru a examina posibilitatea de a aduce capete de acuzare, inclusiv acuzaţii de conspiraţie conform Legii Spionajului din 1917, împotriva lui Julian Assange şi a altora. Reprezentanţi oficiali ai guvernului SUA au spus că investigaţia este „de o natură şi la o scară fără precedent”. În deliberările Marelui Juriu nu sunt prezenţi judecători sau avocaţi ai apărării. De la întocmirea Marelui Juriu, în audieri ale comisiei Congresului s-a ivit sugestia, din partea unor membri ai Congresului SUA, ca Legea Spionajului să fie folosită ca unealtă de atac împotriva jurnaliştilor care „publică în mod conştient scurgeri de informaţie”, lucru care pare să indice că această practică începe să se normalizeze în sistemul juridic al SUA.15

La data publicării acestui text, investigaţia împotriva organizaţiei Wikileaks continuă.16 Mai mulţi oameni au fost constrânşi prin mijloace juridice să depună mărturie. Procedurile judiciare de la procesul lui Bradley Manning,

soldatul acuzat de furnizare de informaţii către Wikileaks, au scos la iveală un dosar FBI al investigaţiei împotriva Wikileaks de peste 42 100 de pagini, dintre care 8.000 se referă la Manning. Bradley Manning a fost reţinut fără proces timp de peste 880 de zile. Raportorul special pentru tortură al ONU, Juan Mendez, a descoperit în mod oficial că Bradley Manning a fost tratat într-o manieră crudă şi inumană, şi care ar putea fi considerată tortură.17

Cereri de asasinare a lui Julian Assange şi grupuri operative Wikileaks declarate public

Investigaţia Marelui Juriu nu este singura strategie de atac împotriva organizaţiei Wikileaks. În luna decembrie a anului 2010, în ajunul publicării dosarului Cablegate, mai mulţi politicieni activi ai guvernului SUA au cerut asasinarea extrajudiciară a lui Julian Assange, inclusiv printr-un atac cu dronă. Senatori ai SUA au etichetat Wikileaks drept o „organizaţie teroristă" şi l-au numit pe Assange un „terorist high-tech" şi un „combatant inamic" într-un „război cibernetic".18

O echipă formată din 120 de angajaţi ai Pentagonului, numită Grupul Operativ Wikileaks sau WTF [*Wikileaks Task Force*\ a fost alcătuită înainte de publicarea dosarelor War Logs şi Cablegate şi dedicată „luării de măsuri" împotriva Wikileaks. Alte grupuri operative similare, declarate public, ale FBI, CIA şi Departamentului de Stat al SUA sunt încă active.19

Cenzură directă într-un proces de cenzură fără precedent a unei publicaţii jurnalistice, guvernul SUA a exercitat presiuni asupra furnizorilor de servicii de internet să sisteze serviciile către Wikileaks.org. În data de 1 decembrie 2010, Amazon a scos site-ul Wikileaks de pe serverele sale de stocare, iar în data de 2 decembrie, serviciul DNS care conducea către domeniul Wikileaks.org

a fost întrerupt. Site-ul Wikileaks a fost menţinut online în timpul acestei perioade ca urmare a unui proces de „mass-mirroring”, prin care mii de susţinători ai Wikileaks au copiat site-ul şi au găzduit propria lor versiune, distribuind adresele IP prin intermediul reţelelor de socializare.20

Administraţia Obama a avertizat funcţionarii statului federal că materialele publicate de Wikileaks rămân clasificate – chiar dacă au fost publicate de unele dintre organizaţiile jurnalistice de top, inclusiv *New York Times* şi *Guardian*. Funcţionarilor li s-a spus că accesarea acestui material, fie de pe Wikileaks.org sau din *New York Timesy* ar fi o violare a siguranţei de stat.21 Unele agenţii ale guvernului, cum ar fi Biblioteca Congresului, Departamentul Comerţului şi armata SUA, au blocat accesul la materialele Wikileaks de pe reţelele lor. Interdicţia nu a fost limitată la sectorul public. Unii angajaţi ai guvernului SUA au avertizat instituţiile academice că studenţii care doresc să urmeze o carieră în serviciul public ar face bine să stea departe, în cercetările lor sau în activitatea Online, de materialele publicate de Wikileaks.

Cenzura financiară: blocada bancară

Wikileaks este finanţată prin donaţii din partea susţinătorilor ei. În luna decembrie a anului 2010, mai multe instituţii bancare de importanţă mondială, printre care VISA, MasterCard, PayPal şi Bank of America au cedat presiunilor neoficiale ale SUA şi au început să refuze serviciile financiare destinate organizaţiei Wikileaks. Au blocat transferurile bancare şi toate donaţiile făcute cu principalele carduri de credit. Deşi acestea sunt instituţii americane, ubicuitatea lor în economia mondială a însemnat că persoanelor care doreau să doneze, atât din America, cât şi din întreaga lume, le era interzisă opţiunea

de a trimite bani către Wikileaks pentru a-i susţine activitatea de publicare.

„Blocada bancară”, după cum a ajuns să fie cunoscută, este impusă în afara unor proceduri juridice sau administrative şi rămâne în vigoare la data publicării celor de faţă. Wikileaks a intentat procese majore în jurisdicţii diferite din toată lumea pentru a opri blocada şi a repurtat o serie de victorii preliminare, iar procesele juridice continuă. Între timp, organizaţia Wikileaks nu are sursă de venit, are costuri mari şi operează de doi ani pe fonduri de rezervă [la data editării – 2012].

Blocada bancară este o afirmare a puterii de a controla tranzacţiile financiare între părţi. Ea subminează în mod direct libertatea economică individuală. În afară de aceasta, ameninţarea existenţială pe care o reprezintă pentru Wikileaks exemplifică o nouă şi înspăimântătoare formă de cenzură economică mondială.22

Câţiva presupuşi asociaţi ai Wikileaks împreună cu susţinători şi însăşi echipa Wikileaks au avut o serie de probleme misterioase cu conturile bancare – de la detaliile contului până la închiderea completă a conturilor.

Hărţuirea lui Jacob Appelbaum şi a lui Jérémie Zimmermann p în data de 17 iulie 2010, Julian Assange a fost invitat să ţină un discurs la conferinţa HOPE a hackerilor din New York. Şi-a anulat discursul, iar în locul său a vorbit Jacob Appelbaum. După acest eveniment, mai multe agenţii ale guvernului au condus o campanie de hărţuire împotriva lui Appelbaum şi a persoanelor apropiate lui. Appelbaum a fost de nenumărate ori reţinut, percheziţionat, i s-a refuzat accesul la o reprezentare juridică şi a fost interogat la punctele vamale de fiecare dată când a intrat sau a ieşit din Statele Unite. I s-a confiscat echipamentul şi i s-au violat drepturile, fiind în

acelaşi timp ameninţat cu violări ulterioare ale drepturilor sale. Zeci de agenţii ale SUA au fost implicate în reţinerea şi hărţuirea sa, de la Departamentul de Securitate Internă, Serviciul pentru Controlul Imigraţiei şi Normelor Vamale, până la armata SUA. Aceste reţineri includ chiar şi refuzul accesului la toaletă ca metodă de forţare a colaborării. Cu toate acestea, Appelbaum nu a fost niciodată acuzat în mod formal, iar reprezentanţii guvernului nu i-au spus niciodată din ce cauză este hărţuit.23

La mijlocul lui iunie 2011, în timp ce se pregătea pentru îmbarcare la aeroportul Dulles din Washington, Jérémie Zimmermann a fost oprit de două persoane care s-au legitimat ca agenţi FBI. Cei doi l-au interogat despre Wikileaks şi l-au ameninţat cu arestarea şi închisoarea.

Appelbaum şi Zimmermann se află pe o listă lungă de prieteni, susţinători sau presupuşi asociaţi ai lui Julian Assange care au fost supuşi hărţuirii şi supravegherii de către agenţii ale SUA, o listă care include avocaţi şi jurnalişti aflaţi în exerciţiul profesiei lor.

Confiscarea fără mandat a arhivelor electronice şi „Cazul somaţiei Twitter”.

În data de 14 decembrie 2010, Twitter a primit o „somaţie administrativă” de la Departamentul de Justiţie al SUA prin care i se ordona să predea informaţii care ar putea fi relevante pentru o investigaţie împotriva Wikileaks. Somaţia ţinea de aşa-numitul „ordin 2703 (d)”, care se referea la o secţiune a Legii Comunicaţiilor Stocate. Conform acestei legi, guvernul SUA îşi atribuie autoritatea de a forţa predarea arhivelor de comunicaţie electronică privată fără necesitatea ca un judecător să emită un mandat de percheziţie – reuşind efectiv să ocolească protecţiile Celui de-al Patrulea Amendament împotriva percheziţiei şi confiscării arbitrare.

Somaţia cerea predarea numelor de utilizator, arhivelor de corespondenţă, adreselor, numerelor de telefon, detaliilor conturilor bancare şi a numerelor cardurilor de credit ale persoanelor presupuse că ar fi asociate cu Wikileaks, inclusiv ale lui Jacob Appelbaum, ale parlamentarei islandeze Brigitta Jonsdottir, ale omului de afaceri şi pionier al internetului Rop Gonggrijp şi ale înseşi organizaţiei Wikileaks. Conform termenilor somaţiei, Twitter avea interdicţia de a le spune acestor persoane de însăşi existenţa ordinului. Cu toate acestea, Twitter a făcut cu succes apel în instanţă împotriva acestei clauze de păstrare forţată a tăcerii şi a câştigat dreptul să informeze persoanele vizate că le erau cerute arhivele.

După ce au fost anunţaţi de către Twitter cu privire la somaţie, în data de 26 ianuarie 2011, Appelbaum, Jonsdottir şi Gonggrijp, reprezentaţi în instanţă de către Kecker şi Van Nest, Uniunea Americană a Libertăţilor Civile şi Electronic Frontier Foundation, au cerut avocaţilor lor să depună împreună un dosar pentru a anula ordinul. Acesta a devenit cunoscut sub numele de „Cazul Somaţiei Twitter”.24 O altă moţiune a fost depusă de avocatul lui Appelbaum, care solicita desigilarea arhivelor încă secrete ale curţii privind încercările guvernului de a strânge datele sale personale de pe Twitter şi pe cele deţinute de alte companii. Ambele moţiuni au fost respinse de către un judecător federal al SUA în data de 11 martie 2011. Reclamanţii au făcut apel.

În data de 9 octombrie 2011, *Wall Street Journal* a dezvăluit faptul că şi furnizorul de servicii de e-mail californian Sonic.net primise o somaţie care cerea datele lui Jacob Appelbaum. Sonic a atacat în instanţă ordinul guvernului şi a pierdut, dar a primit permisiunea să dezvăluie faptul că a fost forţat să predea informaţiile

despre Appelbaum. *Wall Street Journal* a declarat de asemenea că şi Google a primit o somaţie similară, dar nu a specificat dacă Google a contestat decizia în instanţă sau nu.25

În data de 10 noiembrie 2011, un judecător federal a hotărât împotriva lui Appelbaum, Jonsdottir şi Gonggrijp, decretând că Twitter trebuie să predea datele lor Departamentului de Justiţie.26

Reclamanţii au făcut apel din nou în data de 20 ianuarie 2012, încercând să conteste refuzul de a desigila ordinele care ar fi putut fi trimise şi altor companii în afară de Twitter.27 În momentul publicării celor de faţă, procesul continuă.

Intensificarea comunicării *versus* intensificarea supravegherii

JULIAN: Dacă e să ne uităm înapoi în timp, la începutul anilor *90, în momentul amplificării mişcării cypherpunk ca răspuns la interzicerea criptografiei de către stat, mulţi oameni aşteptau de la internet să furnizeze comunicare liberă, necenzurată, spre deosebire de celelalte mijloace de comunicare în masă. Dar activiştii cypherpunk observaseră că, de fapt, alături de această putere, internetul mai avea şi puterea de a supraveghea toate comunicările. Suntem acum în situaţia în care avem o intensificare a comunicării *versus* o intensificare a supravegherii. Intensificarea comunicării înseamnă că avem mai multă libertate faţă de persoanele care încearcă să controleze ideile şi să creeze consimţământ, pe când intensificarea supravegherii intensificată înseamnă exact opusul.

Supravegherea este mult mai evidentă acum decât atunci când surpravegherea în masă era făcută doar de americani, de britanici, de ruşi şi de câteva alte guverne,

cum ar fi cel elveţian sau francez. Acum e făcută de toată lumea şi aproape de fiecare stat, din pricina comercializării supravegherii în masă. Iar acum este totală, pentru că oamenii îşi mută toate ideile politice, comunicarea din familie şi prieteniile pe internet. Aşadar, nu este vorba doar de o supraveghere intensificată a comunicării care exista deja, este vorba de faptul că există mult mai multă comunicare. Şi nu este vorba doar de o înmulţire a volumului comunicărilor, este vorba şi de o înmulţire a tipurilor de comunicare. Toate aceste tipuri noi de comunicare care înainte ar fi fost private sunt acum interceptate în masă.

Există o bătălie între puterea pe care o are această informaţie strânsă de cei care au acces la ea, de aceste state ale informaţiei care încep să se dezvolte în umbră, care fac schimb de informaţie unul cu celălalt, care-şi dezvoltă conexiuni unul cu celălalt şi cu sectorul privat, şi numărul crescând al celor care folosesc internetul ca unealtă comună de comunicare.

Vreau să mă gândesc la felul în care ne vom prezenta ideile. Marea problemă pe care o am din cauză că sunt afundat în fenomenul supravegherii statale şi înţeleg cum s-a dezvoltat industria transnaţională a securităţii în ultimii douăzeci de ani este că sunt mult prea familiarizat cu aceste lucruri şi din această cauză nu înţeleg cum să le văd dintr-o perspectivă a omului obişnuit. Dar acum lumea noastră este lumea tuturor, pentru că toată lumea şi-a aruncat pe internet nucleul intern al vieţii sale. Trebuie să comunicăm cumva lucrurile pe care le ştim cât încă putem.

ANDY: Eu sugerez să nu ne uităm la acest lucru din punctul de vedere al cetăţeanului, ci din punctul de vedere al celor aflaţi la putere. Acum câteva zile mă aflam la o conferinţă ciudată în Washington şi m-am întâlnit cu nişte

tipi care aveau insigna ambasadei Germaniei. I-am abordat şi le-am spus: „A, sunteţi de la ambasada Germaniei”, iar ei au spus: „Nu chiar de la ambasadă, suntem de lângă München”. Am aflat până la urmă că erau dintr-o agenţie de spionaj şi i-am întrebat la bufetul din seara aceea: „Aşadar, care este obiectivul păstrării caracterului secret?” Mi-au spus „Păi, este acela de a încetini procesele pentru a le putea controla mai bine”. Acesta este nucleului tipului acestuia de strângere de informaţii, faptul de a încetini un proces luându-le oamenilor capacitatea de a-l înţelege. A declara secret un lucru înseamnă a limita numărul oamenilor care au cunoştinţele şi deci capacitatea de a influenţa procesul.

Dacă e să ne uităm la internet din perspectiva oamenilor aflaţi la putere, atunci ultimii douăzeci de ani au fost înspăimântători. Ei văd internetul ca pe o boală care le afectează capacitatea de a defini realitatea, de a defini ceea ce se întâmplă, lucruri care mai apoi sunt folosite pentru a defini ceea ce ştiu oamenii despre ceea ce se întâmplă şi capacitatea lor de a interacţiona cu realitatea. Dacă ne uităm, să zicem, la Arabia Saudită, unde, în urma unor împrejurări istorice, liderii religioşi şi cei care deţin majoritatea ţării reprezintă aceiaşi grup, interesul faţă de schimbare este zero. Poate între zero şi minus cinci, mai degrabă – Percep internetul ca pe o boală şi îşi întreabă consilierii: „Aveţi vreun medicament împotriva lucrului ăstuia? Trebuie să ne imunizăm în caz că ne va afecta ţara, în caz că lucrul ăsta numit internet vine peste noi”. Iar răspunsul este supravegherea în masă. Răspunsul este: „Trebuie să-l controlăm în întregime, trebuie să filtrăm, trebuie să ştim tot ce fac”. Iar asta este ceea ce s-a întâmplat în ultimii douăzeci de ani. A existat o investiţie masivă în supraveghere pentru că cei aflaţi la putere s-au

temut că internetul le va afecta tipul de guvernare.

JULIAN: Şi totuşi, în ciuda acestei supravegheri masive, comunicarea în masă a dus la faptul că milioane de oameni au reuşit să ajungă la un consens în mod rapid. Dacă poţi trece foarte repede de la o poziţie normală la una nouă, de consens general, atunci, deşi statul ar putea să vadă ce se întâmplă, nu are destul timp pentru a elabora un răspuns eficient.

Acestea fiind spuse, a existat un protest organizat pe Facebook în 2008, în Cairo. Guvernul Mubar ak a fost luat prin surprindere de acest lucru, iar din această cauză acei oameni au fost depistaţi cu ajutorul Facebook-ului.28 în 2011, într-un manual care a fost unul dintre cele mai importante documente folosite în revoluţia egipteană, pe prima pagină scria: „Nu folosiţi Twitter sau Facebook" pentru a distribui manualul, iar pe ultima pagină scria „Nu folosiţi Twitter sau Facebook" pentru a distribui manualul.29 Cu toate acestea, foarte mulţi cetăţeni egipteni au folosit Twitter şi Facebook. Dar motivul pentru care au supravieţuit a fost acela că revoluţia a avut succes. Dacă nu ar fi avut succes, acei oameni s-ar fi aflat într-o poziţie foarte, foarte neplăcută. Şi să nu uităm că preşedintele Murabak a tăiat internetul în Egipt destul de devreme. Se poate dezbate dacă oprirea internetului a facilitat sau a încetinit revoluţia. Unii cred că a facilitat-o, din cauză că oamenii au trebuit să iasă în stradă pentru a afla ce se petrecea şi, odată ce ai ieşit în stradă, eşti în stradă. Iar oamenii au fost afectaţi în mod direct pentru că nu le mai funcţionau telefoanele mobile şi internetul.

Prin urmare, ca să aibă succes, e nevoie de o masă critică, trebuie să se întâmple rapid şi trebuie să învingă, pentru că dacă nu învinge, aceeaşi infrastructură care a permis ca un consens rapid să se dezvolte va fi folosită

pentru a-i depista şi marginaliza pe toţi acei oameni care au fost implicaţi în crearea consensului.

Deci acesta a fost cazul Egiptului, care, da, era un aliat al SUA, dar care nu face parte din alianţa serviciilor de spionaj vorbitoare de limba engleză formată din SUA, Regatul Unit, Australia, Noua Zeelandă şi Canada. Acum hai să ne imaginăm revoluţia egipteană pornind în Statele Unite – ce s-ar întâmpla cu Facebook şi Twitter? Ar fi preluate de stat. Iar dacă revoluţia nu ar avea succes, ar fi investigate, după cum sunt şi acum, de către CIA şi FBI, pentru a găsi detalii despre cei care au fost participanţii-cheie.

JÉRÉMIE: Este dificil să disociem supravegherea de control. Trebuie să ne ocupăm de ambele. Asta mă interesează pe mine mai mult – controlul internetului, fie că vine din partea guvernului, fie că vine din partea corporaţiilor.

JACOB: Cred că este clar că cenzura este un produs secundar al supravegherii în general, fie că este vorba de autocenzură, fie că e vorba de cenzură tehnică efectivă, şi cred că un aspect important legat de modul în care comunicăm lucrul acesta omului de rând este să o facem nontehnic. De exemplu, dacă am construi drumuri în acelaşi fel în care construim internetul, fiecare drum ar avea camere de supraveghere şi microfoane la care nu ar avea acces nimeni în afară de poliţie sau de cineva care s-ar preface că face parte din poliţie.

JULIAN: La asta se ajunge, Jake, în Regatul Unit.

JACOB: Când construieşti un drum nu e necesar ca fiecare centimetru să fie monitorizat cu o supraveghere perfectă care să fie accesibilă doar unui grup secret de oameni. Explicându-le oamenilor de rând că acesta este felul în care construim drumurile pe internet şi apoi

cerându-le să folosească acele drumuri – acesta este un lucru cu care oamenii obişnuiţi pot rezona, atunci când realizează că constructorii iniţiali ai drumului nu vor fi tot timpul şi cei care-l controlează.

ANDY: Dar unii oameni nici nu construiesc drumuri. Construiesc o grădină şi invită pe toată lumea să stea dezbrăcată. Şi iată-ne ajunşi la Facebook! Este o pledoarie pentru a-i face pe oameni să se simtă confortabil cu dezvăluirea datelor personale.

JACOB: Exact. Oamenii au primit compensaţii pentru că au fost în Stasi – securitatea de stat a fostei Germanii de Est – şi primesc compensaţii şi pentru că fac parte din Facebook. Doar că pe Facebook sunt compensaţi cu credite sociale – şi-o pun cu vecinul – în loc să fie plătiţi în mod direct. Şi este important să ne referim la aspectul uman, pentru că nu este vorba despre tehnologie, este vorba despre controlul prin supraveghere. În anumite aspecte este panopticumul perfect.30

J U LI AN: Mă interesează foarte mult filosofia tehnicii. Tehnica nu înseamnă doar o tehnologie, ci înseamnă, să spunem, consensul majorităţii într-un consiliu, sau structura unui parlament – este interacţiunea sistematizată. De exemplu, am impresia că sistemele feudale s-au născut din tehnologia morilor. Odată ce ai mori centralizate, pentru care e nevoie de investiţii uriaşe şi care pot fi controlate fizic foarte uşor, e firesc să apară relaţii feudale. Cu trecerea timpului se pare că am elaborat tehnici din ce în ce mai sofisticate. Unele dintre aceste tehnici pot fi democratizate, pot fi răspândite tuturor. Dar majoritatea – datorită complexităţii lor – sunt tehnici care se formează în urma unor organizaţii foarte inteconectate, cum ar fi corporaţia Intel. Poate că tendinţa fundamentală a tehnicii este să treacă prin aceste perioade

de descoperire a tehnicii, centralizare a tehnicii, democratizare a tehnicii – când cunoaşterea modului ei de funcţionare se răspândeşte în rândul următoarei generaţii educate. Dar cred că tendinţa generală a tehnicii este să centralizeze controlul în mâinile acelor oameni care controlează resursele fizice ale tehnicilor.

Exemplul suprem al acestui lucru este, cred, ceva de genul unui producător de semiconductoare, unde ai nevoie de o asemenea ordine încât chiar şi aerul trebuie să fie pur, unde ai nevoie de o fabrică în care lurează mii de oameni care trebuie să poarte plase de păr pentru a ţine orice particulă de piele uscată, orice fir de păr departe de procesul de producţie a semiconductoarelor, acesta fiind un proces extrem de complicat, format din mai mulţi paşi. Iar organizaţia producătoare de semiconductoare este în posesia unei cunoaşteri rezultate în urma a milioane de ore de cercetări. Dacă acele lucruri sunt populare, şi sunt, şi dacă se află la baza internetului, atunci codificată în eliberarea internetului se află şi producţia de semiconductoare. Şi codificată în producţia de semiconductoare se află şi capacitatea oricui are controlul fizic asupra producătorului de semiconductoare să extragă concesii uriaşe.

Aşadar, la baza revoluţiei comunicării high-tech – şi a libertăţii pe care am extras-o din aceasta – se află întreaga economie de piaţă modernă, neoliberală, transnaţională şi globalizată. De fapt, ea reprezintă vârful ei. Este maximumul, în termeni de realizări tehnologice, a ceea ce economia neoliberală modernă globalizată poate produce. Internetul se sprijină pe relaţii comerciale extrem de complexe între producătorii de fibră optică, producătorii de semiconductoare, companiile miniere care extrag toate aceste lucruri şi toţi lubrifianţii financiari care înlesnesc

schimbul, tribunalele care impun legile proprietăţii private şi aşa mai departe. Deci este chiar vârful piramidei întregului sistem neoliberal.

ANDY: Referitor la ce spuneai despre tehnică, când Johannes Gutenberg a inventat presa de tipar, ea a fost chiar interzisă ocazional în unele regiuni ale Germaniei şi de aceea s-a răspândit în toată ţara, fiindcă atunci când era interzisă într-o regiune, afacerea se muta într-o altă jurisdicţie.31 Nu am studiat chestiunea în toate detaliile, dar ceea ce ştiu este că Biserica Romano-Catolică a fost deranjată fiindcă se elimina monopolul deţinut de ea pe tipărirea cărţilor, aşa că de îndată ce aveau probleme de ordin juridic, se mutau undeva unde presa nu era interzisă. Într-un fel, acest lucru a ajutat la răspândirea ei.

Internetul a fost puţin diferit, cred, din cauză că pe de-o parte ai maşini care pot fi folosite ca unităţi de producţie, aşa cum a fost, într-un fel, cazul chiar şi cu Commodore 64, deşi majoritatea l-au folosit în alte scopuri.

JULIAN: Deci pe orice mic dispozitiv pe care îl aveai îţi puteai instala propriul software.

ANDY: Da. Şi îl puteai folosi şi pentru a răspândi idei. Dar pe de altă parte, din punct de vedere filosofic, după cum a spus şi John Gilmore – unul dintre fondatorii filialei americane a Electronic Frontier Foundation – la începutul anilor *90, când internetul atinsese întinderea globală: „Reţeaua consideră cenzura ca fiind dăunătoare şi o ocoleşte”.32 După cum ştim astăzi, această afirmaţie a fost un amestec de interpretare tehnică şi de viziune optimistă de impact, un fel de năzuinţă nerealistă şi profeţie auto-împlinită.

JULIAN: Dar a fost adevărat pentru Usenet, care este un sistem de e-mail de grup, dacă vreţi, care a apărut acum treizeci de ani. Pentru a explica Usenet într-o

manieră simplă, imaginaţi-vă că nu există nicio diferenţă între oameni şi servere şi că fiecare persoană are propriul său server Usenet. Se scrie ceva şi se trimite către unul sau doi oameni. Aceştia (în mod automat) verifică dacă au deja mesajul. Dacă nu-l au deja, îl preiau şi-l trimit tuturor celor cu care sunt conectaţi. Şi aşa mai departe. În consecinţă, mesajul ajunge la toată lumea şi toată lumea primeşte, într-un final, o copie. Dacă una dintre persoane cenzurează, ea este pur şi simplu ignorată, nu schimbă cu nimic situaţia. Mesajul continuă să se răspândească prin intermediul tuturor persoanelor care nu cenzurează. Gilmore vorbea despre Usenet, nu vorbea despre internet. Şi nu vorbea nici despre pagini web.

ANDY: Deşi ceea ce spui este corect, interpretarea cuvintelor sale şi impactul lor pe termen lung au fost de natură să producă oameni care se percep pe ei înşişi ca fiind internetul. Oamenii spuneau: „Ok, există cenzură, o vom ocoli”, în timp ce politicianul fără pricepere tehnică se gândea: „Ce rahat, există o nouă tehnologie care ne limitează controlul asupra sferei de informaţii”. Deci cred că Gilmore, care a fost unul dintre premergătorii mişcării cypherpunk, a făcut un lucru foarte bun ducând lucrurile în această direcţie care a inspirat întreaga manieră cripto-anarhistă de a avea propria formă de comunicare anonimă fără a te teme că vei fi urmărit.

JÉRÉMIE: Eu văd o diferenţă în cazul a ceea ce descriem noi ca fiind răspândirea tehnologiei, pentru că în cazul morii sau al presei de tipar trebuia doar să priveşti una din cele două pentru a înţelege cum funcţionează, pe când acum proiectăm controlul din ce în ce mai mult în interiorul tehnologiei. Controlul este încorporat în tehnologie. Dacă ar fi să te uiţi la un computer modern, în cele mai multe cazuri nici nu ai fi în stare să-l deschizi şi să

înveţi toate componentele. Şi toate componentele se află în cutiuţe mici – nu poţi să ştii ce face fiecare.

ANDY: Din cauza complexităţii?

JÉRÉMIE: Din cauza complexităţii, dar şi din cauză că tehnologia ca atare nu este făcută pentru a fi înţeleasă. Aşa stau lucrurile în cazul tehnologiei proprietare.33 Cory Doctorow o descrie în „The War on General-Purpose Computing”.34 Acolo unde computerul este un dispozitiv generalist, poţi face totul cu el. Poţi procesa orice informaţie ca imput; o poţi transforma în orice ca output. Şi construim din ce în ce mai mult aparate care sunt astfel de computere cu scop generalist, dar a căror utilizare e restricţionată doar la a fi GPS-uri sau telefoane sau playere MP3. Construim din ce în ce mai multe dispozitive în care controlul este deja încorporat, pentru a-i interzice utilizatorului să facă anumite lucruri.

JULIAN: Controlul este integrat în dispozitiv pentru a împiedica oamenii să înţeleagă dispozitivul şi să-l modifice, dându-i alt scop decât cel pentru care l-a proiectat producătorul, dar ceea ce se întâmplă acum este şi mai rău, pentru că dispozitivul este conectat la reţea.

JÉRÉMIE: Da, astfel încât să poată conţine funcţia de monitorizare a utilizatorului şi a datelor sale. De aceea software-ul liber este atât de important pentru o societate liberă.

ANDY: Sunt complet de acord că avem nevoie de computerul cu scop generalist, dar în dimineaţa asta, când încercam să vin aici de la Berlin, avionul şi-a întrerupt decolarea – este prima oară când mi s-a întâmplat lucrul acesta. Avionul a tras pe dreapta, iar căpitanul ne-a spus: „Doamnelor şi domnilor, am avut o defecţiune la sistemele electronice, aşa că am decis să ne oprim şi să repomim sistemele”. Şi chiar m-am gândit: „Rahat, parcă ar fi

restartarea la Windows, Control Alt Delete – poate funcţionează!” Aşa că nu aş fi foarte nemulţumit dacă am avea un computer cu scop unic pe avion care să facă doar asta şi să o facă foarte bine. Dacă stau într-o maşinărie zburătoare nu vreau ca piloţii să fie distraşi jucându-se Tetris sau ca avionul să fie infectat cu Stuxnet sau mai ştiu eu ce.35

JÉRÉMIE: Avionul ca atare nu-ţi procesează datele personale, nu are niciun control asupra vieţii tale.

ANDY: Păi o maşină zburătoare are control asupra vieţii mele pentru o vreme.

JACOB: Cred că putem descrie cel mai bine argumentul lui Cory spunând că nu mai există maşini, nu mai există avioane, nu mai există aparate auditive; există computere cu patru roţi, computere cu aripi şi computere care te ajută să auzi. Şi o chestiune importantă nu este aceea dacă sunt sau nu computere cu scop unic, ci dacă putem verifica sau nu că fac lucrul pe care spun că îl fac, şi dacă înţelegem sau nu cât de bine îl fac. Deseori unele persoane încearcă să susţină că au dreptul să ţină aceste lucruri sub cheie, păstrându-le secrete, şi fie proiectează calculatoare complexe, fie ne pun piedici de ordin juridic în calea înţelegerii lor. Acest lucru este periculos pentru societate, fiindcă ştim că oamenii nu acţionează tot timpul în interesul nostru comun, după cum ştim şi că oamenii greşesc – nu din răutate –, astfel că ţinerea acestor lucruri sub cheie este foarte periculoasă din mai multe puncte de vedere, unul dintre acestea fiind faptul că suntem imperfecţi. Aceasta este realitatea. Faptul de a avea acces la schemele sistemelor care ne guvernează viaţa este unul din motivele pentru care software-ul liber este important, dar este de asemenea motivul pentru care hardware-ul liber este important. Ne îmbunătăţeşte capacitatea de a

face liber investiţii sustenabile, de a îmbunătăţi sistemele pe care le folosim şi de a afla dacă sistemele acestea funcţionează cum ar trebui. Dar dincolo de libertate, acesta este şi motivul pentru care e important să înţelegem aceste sisteme, pentru că atunci când nu le înţelegem, există o tendinţă generală de a ceda în faţa autorităţii, în faţa oamenilor care le înţeleg şi care pot să le controleze, chiar dacă aceştia nu înţeleg esenţa lucrului ca atare. De aceea se vorbeşte atât despre războiul cibernetic – din cauză că unii oameni care par să aibă autoritatea în ceea ce priveşte războiul încep să vorbească despre tehnologie ca şi cum ar înţelege-o. Astfel de oameni vorbesc deseori despre războiul cibernetic şi niciunul dintre ei, nici măcar unul, nu vorbeşte despre menţinerea păcii prin mijloace cibernetice sau de orice ar ţine de menţinerea păcii. Vorbesc tot timpul despre război din cauză că asta e treaba lor şi încearcă să controleze procesele tehnologice şi juridice pentru a-şi promova interesele proprii. Aşadar, când nu deţinem controlul asupra tehnologiei noastre, astfel de persoane vor dori să o folosească pentru scopurile lor, în speţă pentru război. Iar asta e reţeta pentru nişte lucruri destul de înspăimântătoare – aşa cred că s-a ajuns la Stuxnet –, iar unele persoane altminteri rezonabile vor sugera, în timp ce SUA se află în război, că astfel de tactici ar putea cumva să prevină războiul.

Acest argument este, poate, unul rezonabil pentru o ţară care nu invadează în mod activ alte naţiuni, dar cu greu poate fi unul credibil în contextul unei naţiuni implicate în invadări multiple şi concomitente.

Militarizarea spaţiului cibernetic

JULIAN: Am observat că ne aflăm acum într-un proces de militarizare a spaţiului cibernetic, în sensul unei

ocupaţii militare. De fiecare dată când comunicăm pe internet, când comunicăm folosind telefoanele mobile, care acum sunt legate la internet, comunicările noastre sunt interceptate de organizaţii militare de spionaj. Este ca şi cum ai avea un tanc în dormitor. Între tine şi soţie se află un soldat atunci când vă trimiteţi SMS-uri. În ceea ce priveşte comunicările noastre, trăim cu toţii sub legea marţială, doar că nu putem vedea tancurile – dar ele sunt aici. În acest sens, internetul, care ar fi trebuit să fie un spaţiu civil, a devenit un spaţiu militarizat. Dar internetul este spaţiul nostru, pentru că îl folosim cu toţii pentru a comunica unii cu ceilalţi şi cu membrii familiei noastre. Comunicările cele mai intime din vieţile noastre private se fac acum pe internet. Deci, de fapt, vieţile noastre private au intrat într-un spaţiu militarizat. Este ca şi cum ai avea un soldat sub pat. Aceasta este militarizarea vieţii civile.

JACOB: Chiar înainte să vin aici mi s-a propus să fiu antrenor al echipei Laboratorului de Cercetare în domeniul Securităţii şi Confidenţialităţii al Universităţii din Washington pentru concursul Pacific Rim Collegiate Cyber Defense. În ultimul moment mi s-a propus să fiu consilier. Am petrecut o groază de timp concurând într-o competiţie de război cibernetic în care SPAWAR, o ramură civilă a marinei SUA, ce include şi servicii constând în teste de penetrare şi care face atât hacking ofensiv, cât şi hacking defensiv, era ceea ce se numeşte de obicei Echipa Roşie.36 Ceea ce fac ei este să-i atace pe toţi cei care joacă, iar sarcina fiecărei echipe este să-şi apere sistemele informatice pe care le-au primit la începutul competiţiei, fără să ştie dinainte ce se va întâmpla. Nu ştii ce fel de sisteme vei apăra şi nici măcar nu este clar cum funcţionează punctajul la început, aşa că încerci să dai tot ce ai mai bun şi să speri.

JULIAN: Eşti sigur că ăsta e un joc? Poate nu e un joc!

JACOB: Nu, primeşti doar nişte calculatoare pe care trebuie să le aperi, şi alţii încearcă să le spargă şi să preia controlul* sistemelor. Este ca un joc de-a Prinde Steagul la o conferinţă de hackeri sau ceva de genul, şi e interesant pentru că băieţii ăştia au multe instrumente, au scris software.37

JULIAN: Dar care e scopul jocului ăstuia – din perspectiva marinei SUA?

JACOB: Păi, în cazul lor, sponsorizează asta pentru că vor să formeze astăzi războinicii cibernetici de mâine şi, de exemplu, ţi-am adus un carneţel de la CIA, pentru că recrutau. Era un tip acolo care se numea Charlie – Charlie de la CIA –, care explica că dacă vrei să vii să te angajezi la CIA, aceasta este o ocazie foarte bună pentru a lucra în lumea reală. Şi erau acolo şi oamenii de la SPAWAR, şi era şi Microsoft care recruta. Ideea era să antrenezi toţi acei oameni, toate acele echipe, să ajungă la Campionatul Naţional şi să câştige şi să „apere ţara”, iar apoi să poată ajunge să facă hacking ofensiv ca războinici cibernetici, nu doar ca apărători cibernetici. Am avut un punctaj de 4.000 de puncte, care a fost punctajul cumulat al echipelor de pe locurile doi, trei şi patru. A fost de fapt chiar mai mare decât toate punctele lor puse împreună.

JULIAN: Da, da, da.

JACOB: Nu a fost mulţumită mie – discursul meu de motivare a >

fost un fel de „Băieţi, cel mai mare întuneric este întotdeauna fix înainte să se facă beznă” – şi nici nu sunt prea bun la antrenat – băieţii ăştia sunt foarte buni. Dar *x* fost interesant pentru că modul în care era prezentată toată chestia era în termeni de război, aşa că ziceau: „Hei,

vrem să vă auzim strigătul de război”. Îţi venea să zici: „Poftim? Cum adică?” Asta spuneau în timpul prânzului, de exemplu, când luau o pauză de la apărarea sistemelor noastre. Formulau totul în termeni de atacare a sistemelor şi de război cibernetic şi de măreţie a acestui fel de a gândi. Şi, foarte interesant, în afară de echipa cu care lucram eu, am avut impresia că mulţi dintre acei oameni aveau mari bătăi de cap, pentru că nu erau instruiţi să folosească Arta Războiului – era mai degrabă ca la Cupa Sysadmin, oameni care apără sisteme – şi mi s-a părut dezgustător.38 M-am simţit foarte bizar, pentru că toţi oamenii ăştia care aveau experienţa războiului veneau cu o perspectivă de război, dar nu predau strategie, erau foarte concentraţi pe retorica apărării acestor sisteme sau a atacului acestor sisteme şi aveau atâta război în cap încât chiar încercau să incite pe toată lumea într-un soi de fervoare patriotică. Nu promovau gândirea creativă sau vreun fel de cadru pentru analiză independentă; îndemnau la o mentalitate-a-angrenajului-într-o-maşinărie, a cuiva care urmează ordinele pentru binele naţiunii. Nu mai avusesem o asemenea experienţă până atunci. Mi s-a făcut rău şi majorităţii celor din echipa mea le-a fost greu s-o digere sau măcar s-o ia în serios.

JULIAN: Crezi că e un antrenament standard al marinei SUA şi că încearcă acum să-l folosească într-un alt domeniu? Este oare o decizie venită din partea conducerii SUA pe domeniul cibernetic – o decizie strategică internaţională?

ANDY: Mai degrabă ca în cazul naziştilor care aveau acele tabere în care erau antrenaţi copii.

JACOB: *Sie konnen das sagen weil du bist Deutsche*. Poţi să spui asta pentru că eşti neamţ. Nu, nu e aşa. Marina SUA se implică doar din cauză că guvernul SUA

sponsorizează toată chestia asta. Mi-au propus să-i pregătesc pentru că aveau nevoie de cineva care să-i pregătească şi am acceptat pentru că-mi plăceau băieţii implicaţi, studenţii. Dar, de fapt, lucrul se rezumă la faptul că guvernul SUA încearcă să împingă oamenii în chestia asta şi încearcă să o facă dintr-o perspectivă a naţionalismului. Este o competiţie foarte stranie pentru că, pe de-o parte, este bine să ştii cum să-ţi aperi sistemul şi e bine să înţelegi infrastructura pe care se bazează vieţile noastre; dar, pe de altă parte, nu încercau să convingă oamenii să le înţeleagă, încercau să le inducă un soi de fervoare pentru a-i face să le placă genul ăsta de activitate.

ANDY: Din păcate, interesul Statelor Unite în ceea ce priveşte menţinerea securităţii sistemelor este total limitat, pentru că îşi doresc ca sistemele să fie vulnerabile, ca ei să poată prelua controlul asupra lor. Încercarea de a controla criptografia mondială nu a mers atât de departe precum şi-au dorit la început Statele Unite, undeva prin 1998, când David Aarons, subsecretarul SUA însărcinat cu comerţul internaţional, a fost într-un turneu mondial pledând pentru necesitatea accesului guvernului la parolele tuturor.39 Dar criptografia este încă considerată o tehnologie cu o aşa-numită dublă întrebuinţare, iar expprtul său în alte ţări, sub forma produselor pentru utilizatorul final, este limitat prin lege stabilită în cadrul unei convenţii mondiale numite Acordul de la Wassenaar.40 E un lucru care ar putea suna rezonabil, în contextul declarării anumitor naţiuni şi a acţiunilor lor ca fiind „ticăloase”, dar el indică dimensiunea standardului dublu, căci, deocamdată, tehnologia de supraveghere a telecomunicaţiilor nu este reglementată prin controlul exporturilor.41

JULIAN: Andy, tu ai conceput ani de zile telefoane

criptografice. Despre ce fel de supraveghere în masă se poate vorbi referitor la telecomunicaţii? Spune-mi care este vârful tehnologic în ceea ce priveşte industria spionajului/supravegherii en-gros făcute de guvern?

AN DY: Stocarea în masă – care presupune stocarea tuturor telecomunicaţiilor, a tuturor apelurilor vocale, a tuturor datelor de trafic, a tuturor modurilor în care grupurile folosesc Serviciul de Mesaje Scurte (SMS), dar şi a tuturor conectărilor la internet, care în unele cazuri conţin cel puţin serviciile de e-mail. Dacă compari bugetul armatei cu costul supravegherii şi al războinicilor cibernetici, sistemele obişnuite de armament costă mult. Războinicii cibernetici sau supravegherea în masă sunt foarte ieftine comparate chiar şi cu un singur avion. Un avion militar te costă între…

JULIAN: În jur de o sută de milioane.

ANDY: Iar stocarea devine în fiecare an din ce în ce mai ieftină. La Chaos Computer Club am făcut chiar nişte calcule: poţi să stochezi, la o calitate decentă, toate apelurile telefonice făcute într-un an în Germania cu circa 30 de milioane de euro, iar asta include şi cheltuielile administrative, deci doar stocarea ar costa în jur de 8 milioane de euro.42

JULIAN: Şi există chiar companii, cum este VAST – ech în Africa de Sud, care scot aceste sisteme la vânzare la preţul de 10 milioane de dolari pe an.43 „Vă vom intercepta toate apelurile şi vom stoca în masă toate apelurile interceptate”. Dar în ultimii ani s-a făcut o trecere de la interceptarea tuturor comunicaţiilor dintre o ţară şi alta şi selectarea acelor oameni pe care vrei să-i spionezi şi încredinţarea lor în seama altor oameni, la interceptarea tuturor comunicaţiilor şi la stocarea lor permanentă.

AN DY: Ca să dau o explicaţie oarecum istorică a acestui fenomen, pe vremuri erai o ţintă din cauza poziţiei diplomatice, din cauza companiei pentru care lucrai, din cauză că erai suspectat că ai fi făcut ceva sau erai în contact cu oameni care chiar făceau ceva, şi apoi se aplicau măsurile de supraveghere împotriva ta. În ziua de azi pare mult mai eficient să spui „Luăm totul şi triem mai târziu”. Deci chiar au stocare pe termen lung, iar modalitatea cea mai bună de a descrie cele două capitole ale acestei industrii sunt abordarea „tactică” şi abordarea „strategică”. Tactic înseamnă: „În acest moment, în timpul acestei întâlniri, trebuie să interceptăm totul, trebuie să infiltrăm pe cineva cu un microfon sau să avem sisteme de supraveghere prin GSM (Sistem Global pentru Comunicaţiile Mobile) într-o maşină, gata instalate, capabile să intercepteze imediat tot ce se spune, fără să avem nevoie de amestecul operatorului de reţea, fără să avem nevoie să obţinem un mandat de percheziţie sau ceva de genul ăsta de la poliţie, fără să avem nevoie de proceduri juridice – s-o facem pur şi simplu”. Abordarea strategică este să o faci automat, să înregistrezi pur şi simplu totul şi să sortezi după aceea înregistrările, folosind sisteme analitice.

JULIAN: Deci interceptarea strategică este să iei tot ce se transmite printr-un satelit de telecomunicaţii, să iei tot ce trece printr-un cablu de fibră optică.

AN DY: Pentru că nu ştii niciodată când cineva este suspect.

JACOB: Există în Statele Unite ceva ce se numeşte cazul NSA AT & Tal doilea caz: Hepting *vs* AT & T. în oraşul Folsom din California, Mark Klein, un fost tehnician al uriaşei companii de telecomunicaţii AT & T, a scos la iveală faptul că NSA, Agenţia Naţională de Securitate SUA,

capta toate datele pe care i le putea oferi AT & T Pur şi simplu le lua en gros – atât date, cât şi apeluri telefonice –, aşadar de fiecare dată când ridicam receptorul sau mă conectam la internet în San Francisco în timpul perioadei despre care a vorbit Mark Klein, ştim că pe pământ american, împotriva cetăţenilor SUA, NSA primea totul.44 Sunt sigur că au folosit datele interceptate respective în investigaţii împotriva persoanelor din Statele Unite, lucru care ridică tot soiul de probleme constituţionale interesante, deoarece reţin datele pentru totdeauna.

JÉRÉMIE: Mai este şi exemplul Eagle, sistemul vândut Libiei lui Gaddafi de către compania franceză Amesys, iar pe documentul comercial scria „Mecanism de interceptare naţională”. Este o cutie mare pe care o pui undeva şi stai şi asculţi conversaţiile întregului popor.45

JULIAN: Acum zece ani, lucrurile acestea erau văzute drept ceva de domeniul fantasticului, un lucru în care credeau doar oamenii paranoici, dar costurile interceptării în masă au scăzut în aşa măsură încât până şi o ţară ca Libia, cu resurse relativ puţine, a ajuns să o facă, cu tehnologie franceză. În realitate, majoritatea ţărilor au ajuns în acest punct, în ceea ce priveşte interceptarea. Următorul mare pas va fi eficienţa cu care vor fi înţelese informaţiile interceptate şi stocate, şi eficienţa reacţiei faţă de acestea. Acum are loc, în multe ţări, interceptarea strategică a întregului trafic care intră sau iese din ţară, dar acţiunile care urmează acestei interceptări, cum ar fi blocarea automată a conturilor bancare, sau desfăşurarea forţelor poliţiei, sau marginalizarea anumitor grupuri, sau emanciparea altora, sunt lucruri până la care mai e încă un pas. Siemens vinde o platformă pentru agenţii de spionaj care produce acţiuni automate. Aşadar, când persoana ţintă A se află la un anumit număr de metri de persoana

ţintă B conform interceptării telefoanelor mobile, iar persoana ţintă A primeşte un e-mail care menţionează ceva – un cuvânt-cheie – se declanşează acţiunea. pe punctul de a se produce.

Combaterea supravegherii totale cu ajutorul legilor omului

JÉRÉMIE: Prin urmare, acum este fapt real acela că tehnologia permite supravegherea totală a tuturor comunicaţiilor. Apoi mai este şi cealaltă faţă a monedei, anume ce facem cu ceea ce interceptăm. Putem admite că pentru ceea ce numeşti supraveghere tactică există utilizări legitime – diverşi investigatori care anchetează ticăloşi sau reţele de ticăloşi şi aşa mai departe s-ar putea să aibă nevoie, sub supravegherea unei autorităţi judiciare, să se folosească de astfel de instrumente –, dar întrebarea este: unde trasăm limita acestei supravegheri judiciare, unde trasăm limita controlului pe care-l pot avea cetăţenii asupra folosirii acestor tehnologii? Este o problemă de politică. Şi când ajungem la problemele acestea de politică, se întâmplă ca unii politicieni să fie rugaţi să semneze ceva fără să înţeleagă tehnologia de la bază, şi cred că noi, ca cetăţeni, avem un rol, nu doar să explicăm, inclusiv politicienilor, cum funcţionează tehnologia, ci şi să intrăm în dezbaterile politice din jurul folosirii acestor tehnologii. Ştiu că în Germania a existat o mişcare masivă împotriva reţinerii generalizate de date, care a dus la răsturnarea Legii Reţinerii Datelor în faţa Curţii Constituţionale.46 Există acum în Uniunea Europeană o dezbatere despre revizuirea Directivei Reţinerii Datelor.47

ANDY: Descrii aici teoria statului democratic, care, desigur, trebuie să filtreze nişte ticăloşi ici şi colo şi să le asculte telefoanele, pe baza unei hotărâri judecătoreşti şi cu supraveghere juridică, în scopul asigurării că procedura

se face cum se cuvine. Problema este că autorităţile trebuie să acţioneze în concordanţă cu legea. Dacă nu fac asta, atunci la ce mai sunt bune? Mai cu seamă în cazul abordării acesteia strategice, unele state democratice europene cumpără masiv aparate care le permit să acţioneze tocmai în afara legii în ceea ce priveşte interceptarea, pentru că nu au nevoie de o hotărâre judecătorească, au nevoie doar să pornească aparatele şi să o facă, iar tehnologia asta nu poate fi controlată.

JULIAN: Dar sunt oare două abordări în ceea ce priveşte supravegherea în masă a statului: legile fizicii şi legile omului? Una este să foloseşti legile fizicii construind efectiv instrumente care previn interceptarea. Cealaltă este să pui în aplicare prin lege controale democratice pentru a te asigura că oamenii vor avea nevoie de mandate şi aşa mai departe şi să încerci să câştigi puţină responsabilizare legislativă. Dar interceptarea strategică nu poate face parte din asta, nu poate fi limitată în mod semnificativ prin legislaţie. Interceptarea strategică se ocupă cu interceptarea *oricui*, indiferent dacă e vinovat sau nevinovat. Trebuie să ne amintim ca tine

de nucleul cercurilor conducătoare faptul de a efectua asemenea supraveghere. Va exista întotdeauna o lipsă de voinţă politică de a dezvălui acţiunile de spionaj ale statului. Iar tehnologia este în sine atât de complexă, iar folosirea sa în practică atât de secretă, încât nu poate exista o supraveghere democratică semnificativă.

ANDY: Sau îţi spionezi propriul parlament.

JULIAN: Dar alea sunt scuze – mafia şi spionajul străin –, sunt scuze pentru ridicarea unui astfel de sistem, astfel ca oamenii să accepte.

JACOB: Cei Patru Călăreţi ai Apocalipsei Informatice:

pornografia infantilă, terorismul, spălarea de bani şi Lupta împotriva unor Droguri.

JULIAN: Odată ce ai instalat acest sistem de supraveghere, având în vedere că este complex, având în vedere că este conceput să funcţioneze în secret, nu este oare adevărat că el nu poate fi reglementat politic? Cred că, exceptând state foarte mici ca Islanda, dacă nu există circumstanţe revoluţionare nu va fi posibil să controlezi interceptarea în masă cu legislaţie şi politici publice. Pur şi simplu nu se va întâmpla lucrul acesta. Este mult prea ieftin şi prea uşor să ocoleşti răspunderea politică şi să interceptezi realmente. Suedia a avut în 2008 un proiect de lege privind interceptarea, cunoscut sub numele de FRA-lagen, care prevedea că agenţia suedeză de spionaj, FRA, putea intercepta în masă, în mod legal, toate comunicaţiile care treceau prin ţară şi le putea trimite Statelor Unite, cu unele limitări.48 Dar cum poţi să pui în aplicare acele limitări odată ce ai instalat sistemul de interceptare, iar organizaţia care-l foloseşte este o agenţie secretă de spionaj? E imposibil. Iar, în realitate, unele cazuri care au ieşit la iveală au arătat că FRA încălcase legea cu mai multe prilejuri. Multe ţări o fac în afara legii, fără absolut nicio acoperire legislativă. Deci suntem cumva norocoşi dacă, la fel ca în exemplul suedez, s-a decis, pentru propria protecţie faţă de urmărirea în instanţă, să se intre în legalitate schimbând legea. Iar aceasta este situaţia celor mai multe ţări – se face interceptare en gros, iar de fiecare dată când se fac propuneri legislative, se fac pentru a-i proteja pe cei care o fac.

Tehnologia aceasta este foarte complexă; de exemplu, în cazul dezbaterii din Australia şi din Regatul Unit în ceea ce priveşte legislaţia propusă pentru a intercepta toate metadatele, majoritatea populaţiei nu

înţelege valoarea metadatelor şi nici măcar cuvântul în sine.49 A intercepta toate metadatele înseamnă că trebuie să construieşti un sistem care interceptează fizic toate datele, iar apoi aruncă la gunoi totul în afară de metadate. Dar nu poţi avea încredere într-un astfel de sistem. Nu există nicio modalitate prin care să-ţi dai seama dacă nu cumva interceptează şi stochează de fapt toate datele, neavând ingineri poate pricepuţi şi autorizaţi să meargă şi să verifice exact ce se petrece, şi nu există voinţă politică pentru a acorda accesul în aces sens. Problema se înrăutăţeşte, din cauză că secretele şi complexitatea sunt un amestec toxic. Tăinuit prin complexitate. Tăinuit prin caracterul secret. Fenomenul interceptării este incontrolabil prin însăşi natura sa. Incontrolabilitatea este o caracteristică a lui. Este periculos prin însuşi felul în care a fost conceput.

JEREMIE: Eu nu spun că abordarea politică poate funcţiona. Spun că aceasta este teoria despre cum ar trebui să funcţioneze un sistem democratic şi, într-adevăr, chiar şi cu această teorie ai serviciile secrete, cărora le este permis să nu respecte regulile pentru forţele de poliţie şi investigatorii standard. Deci chiar dacă limităm cum trebuie comportamentul investigatorilor standard, ar exista alţi oameni care ar putea folosi aceste tehnologii. Dar adevărata întrebare este aceea dacă ar trebui sau nu să reglementăm cumpărarea şi deţinerea acestor tehnologii, în loc să reglementăm folosirea lor.

JULIAN: Vorbim despre echipamente pentru interceptare în masă, care pot intercepta jumătate de ţară sau un oraş.

JÉRÉMIE: Da. La fel ca o armă nucleară: nu poţi vinde uşor o armă nucleară, iar unele ţări ar putea să-şi dorească să construiască una, dar au probleme. Când

vorbim despre sisteme de armament, tehnologia este cea care este reglementată, nu folosirea ei. Cred că dezbaterea ar putea fi dacă aceste tehnologii ar trebui sau nu considerate ostile.

JACOB: Depinde. Când sunt arme – şi nu există niciun dubiu că echipamentul pentru supraveghere este o armă în ţări cum ar fi Siria sau Libia –, simt folosite în mod special pentru a supraveghea persoane din interese politice. Compania franceză Amesys a supravegheat persoane în Regatul Unit cu tehnologie franceză care ar fi fost ilegală în Franţa, şi au vândut-o în cunoştinţă de cauză.50

ANDY: Şi nu ar face asta niciodată, nu?

JACOB: Păi, compania Amesys a fost prinsă împreună cu propriile documente interne în The Spy Files.51 Dacă e să vorbim despre lucrurile acestea în termeni de armament, trebuie să ne amintim că nu este ca şi cum ai vinde unei anumite ţări un camion. Este ca şi cum ai vinde unei anumite ţări un camion, un mecanic şi o echipă care intră în camion şi ia în vizor în mod selectiv oameni pe care mai apoi îi împuşcă.

JULIAN: Este ca şi cum ai vinde o întreagă armată de camioane.

ANDY: Este interesant că criptografia e reglementată. Există Acordul de la Wassenaar, cu aplicare internaţională, care stipulează că nu poţi exporta acelor ţări care au fost declarate ticăloase sau, din diverse motive, problematice, tehnologie de criptare care ajută la protejarea împotriva tehnologiei de supraveghere. Dar dacă comercializezi echipament de supraveghere, *poţi* să-l vinzi pe plan internaţional. Pentru acesta nu există restricţii la export. Iar motivul, aş spune eu, este pur şi simplu acela că până şi guvernele democratice au un interes propriu, şi anume să controleze. Şi chiar dacă faci

afaceri cu ţări ticăloase şi le trimiţi echipament de supraveghere pentru a face cu el lucruri ticăloase, tot vei avea de câştigat, pentru că vei afla lucrurile pe care le ascultă ei, lucrurile de care se tem, care sunt cei mai importanţi oameni care se opun guvernului şi care organizează evenimente politice şi aşa mai departe. Deci vei putea prevedea evenimente viitoare, vei putea sponsoriza acţiuni şi aşa mai departe. Iată-ne ajunşi în jocul foarte murdar reprezentat de ceea ce se întâmplă între ţări, iar acesta este, de fapt, motivul pentru care sistemele de supraveghere nu sunt reglementate.

JULIAN: Aş vrea să vorbesc despre analogia dintre sistemele de supraveghere şi armele de distrugere în masă. A fost o chestiune de fizică faptul că s-a putut construi bomba atomică, iar când a fost construită o bombă atomică s-a produs o schimbare geopolitică şi s-a schimbat viaţa multor oameni – în moduri diferite, poate unele dintre ele pozitive, altele la graniţa apocalipsei totale. O mişcare legislativă a aplicat controale, iar până acum, aceste controale ne-au apărat de un război nuclear, excepţie făcând Japonia. Dar este uşor să-ţi dai seama când astfel de arme sunt folosite şi când nu.

Odată cu creşterea sofisticării şi cu scăderea costului supravegherii în masă din ultimii zece ani, am ajuns acum într-o situaţie în care populaţia globală se dublează o dată la aproximativ douăzeci şi cinci de ani – iar capacitatea de supraveghere se dublează o dată la optsprezece luni. Curba supravegherii domină curba populaţiei. Nu există nicio scăpare directă. Am ajuns în situaţia în care cu doar 10 milioane de dolari îţi poţi cumpăra o unitate în care să stochezi permanent interceptările în masă ale unei ţări de dimensiuni medii. Deci mă întreb dacă nu cumva avem nevoie de un răspuns echivalent. Aceasta este o

ameninţare serioasă la adresa democraţiei şi libertăţii în toată lumea şi reclamă un răspuns, la fel cum ameninţarea războiului atomic a reclamat un răspuns masiv, pentru a încerca să o controlăm, cât încă se mai poate.

ANDY: Eu am văzut în Libia cum mişcarea democratică a dat peste staţiile de supraveghere, a luat arhivele, a adus dovezi că unele companii occidentale au susţinut regimul lui Gaddafi în înăbuşirea acţiunilor politice, iar apoi noul guvern a preluat exact acele instalaţii, care acum lucrează din nou la capacitate maximă.52 Aşadar, deşi sunt de acord că ar fi o idee bună să controlăm această tehnologie, sunt puţin sceptic în ceea ce priveşte raportul dintre interesele cetăţenilor şi interesele oamenilor aflaţi la putere. Nici nu le-aş numi neapărat guverne, pentru că oricine poate să asculte toate apelurile telefonice va putea să facă diverse chestii. Este vorba şi despre preţul acţiunilor – poţi beneficia mult din punct de vedere economic dacă ştii ce se petrece.

J U LI AN: Ţările cu legislaţie ce reglementează interesele agenţiilor principale de spionaj – agenţii ca NSA în Statele Unite, GCHQ (Governement Communications Headquarters) în Regatul Unit, DSD (Defence Signals Directorate) în Australia – au schimbat respectiva legislaţie pentru a include spionajul economic. De pildă, să spunem că dacă Australia şi SUA s-ar afla în concurenţă într-o tranzacţie cu grâu, i-ar spiona pe toţi cei care sunt implicaţi în vânzare. Acest lucru se întâmplă deja de multă vreme, de cel puţin zece ani în mod public – dar e acceptat pentru că oamenii l-ar face oricum. A început cu vânzări de armament, caz în care ai companii ca Lockheed Martin, Raytheon şi Northrup care fac comerţ cu arme şi care construiesc şi sisteme de interceptare în masă, pentru că aceste grupuri sunt apropiate la nivel de patronaj. Au

primit favoruri de la prieteni şi au introdus interceptarea vânzărilor de arme sub criterii de siguranţă naţională. Dar acum se aplică în cazul a orice ar putea aduce beneficii unei ţări din punct de vedere economic, adică la aproape orice.

JACOB: O bună analogie pe care au adus-o în discuţie nişte participanţi la Congresul Chaos Communication, din decembrie 2011, a fost conceptul de a trata tehnologia supravegherii, mai cu seamă tehnologia supravegherii tactice, dar şi tehnologia supravegherii strategice ca pe o mină.53 Cred că este o analogie puternică. Doar pentru că e posibil nu înseamnă neapărat că e şi inevitabil să continuăm pe drumul acesta şi nu înseamnă că trebuie să ajungem în punctul în care fiecare persoană va fi monitorizată.

Există totuşi unele considerente economice care sunt împotriva noastră. De exemplu, cineva mi-a explicat felul în care funcţiona sistemul norvegian de telefonie, anume acesta avea, practic, un contor care în funcţie de cât de departe sunai se învârtea mai repede sau mai încet. Dar nu era legal pentru compania norvegiană de telefonie să arhiveze sau să ţină un registru cu metadatele apelului efectuat, cum ar fi numărul apelat, tocmai din cauza preocupărilor legate de confidenţialitate care dominau perioada celui de-al Doilea Război Mondial. Deci ar fi posibil să construim tehnologia într-o manieră care protejează confidenţialitatea, dar care permite totuşi o abordare de piaţă, ce permite totuşi contribuţii economice. Cu toate acestea, nu putem câştiga, de pildă, cu tehnologiile GSM (de telefonie mobilă). În momentul de faţă, felul în care sunt configurate aceste sisteme, nu doar în termeni de facturare, ci şi în termeni de arhitectură, semnifică faptul că ele nu au confidenţialitate a amplasării,

nu au confidenţialitate a conţinutului.

JULIAN: Telefonul mobil este un instrument de urmărire care face şi apeluri.

JACOB: Exact. Bunăoară, atunci când spunem că toate persoanele din Lumea a Treia sunt spionate, ce înseamnă asta în mod realist? înseamnă că sistemele lor de telefonie, adică legătura lor cu restul lumii, sunt instrumente de spionaj în momentul în care cineva decide să se folosească de informaţiile adunate în acel mod.

ANDY: Am văzut că statele africane primesc o întreagă infrastructură pentru internet, inclusiv cabluri de fibră optică şi comutatoare pentru *backbone-ul* reţelei, cadou de la chinezi.

JACOB: Cadou de la ZTE sau ceva de genul ăsta? 54

ANDY: Da, şi, desigur, chinezii sunt interesaţi de datele acelea, aşa că nu trebuie să fie recompensaţi cu bani, ci îşi vor lua recompensa sub formă de date, noua monedă.

Spionajul sectorului privat

JÉRÉMIE: Supravegherea sponsorizată de stat este într-adevăr o problemă majoră, care pune sub semnul întrebării structura însăşi a tuturor democraţiilor şi modul în care funcţionează ele, dar există şi supraveghere privată şi, posibil, strângere masivă de informaţii făcută în privat. Uitaţi-vă la Google. Dacă sunteţi un utilizator Google standard, Google ştie cu cine comunicaţi, pe cine cunoaşteţi, ce căutaţi, poate şi orientarea voastră sexuală şi credinţele religioase şi filosofice.

ANDY: Ştie mai multe despre tine decât ştii tu însuţi.

JÉRÉMIE: Mai mult decât mama ta şi poate chiar mai mult decât tine însuţi. Google ştie când eşti online şi când nu.

ANDY: Ştii ce ai căutat acum doi ani, trei zile şi patru

ore? Tu nu ştii; Google ştie.

JÉRÉMIE: De fapt, încerc să nu mai folosesc Google, tocmai din aceste motive.

JACOB: Este un fel de Omoară-ţi Televizorul în varianta secolului XXI.55 Un protest eficient, doar că efectul de reţea împiedică protestul tău să funcţioneze.56 Omoară-ţi televizorul, omule.

J EREM IE: Păi nu este un protest, este mai degrabă felul meu personal de a vedea lucrurile.

ANDY: Am văzut nişte filmări foarte frumoase cu oameni care-şi aruncau televizoarele din clădiri de câte trei etaje.

JEREM IE: Nu e vorba doar de supravegherea sponsorizată de stat, e vorba despre chestiunea confidenţialităţii, de felul în care datele sunt administrate de terţi şi de măsura în care oamenii au cunoştinţă despre ceea ce se face cu datele. Eu nu folosesc Facebook, deci nu ştiu prea multe despre el. Dar acum, cu Facebook-ul, poţi vedea comportamentul unor utilizatori care sunt foarte încântaţi să ofere orice fel de date personale, şi poţi să-i învinovăţeşti că nu ştiu care este limita dintre privat şi public? Acum câţiva ani, înainte de tehnologiile digitale, oamenii care aveau o viaţă publică erau fie in show-business, fie în politică sau în jurnalism, iar acum fiecare are posibilitatea unei vieţi publice prin simpla apăsare a unui buton de distribuire. A „distribui” înseamnă a face ceva public, înseamnă a acorda accesul către acele date restului lumii – şi, desigur, când vezi adolescenţi care postează poze cu ei beţi sau mai ştiu eu ce, s-ar putea ca ei să nu vadă lucrurile în acest fel, anume că înseamnă tot restul lumii, poate pentru o perioadă foarte, foarte lungă. Facebook funcţionează ca afacere prin estomparea graniţelor dintre confidenţialitate, prieteni şi publicitate.

Şi îţi şi stochează datele, atunci când tu crezi că sunt destinate doar prietenilor tăi şi oamenilor care-ţi sunt dragi. Deci oricare e gradul în care doreşti să îţi fie publice datele, de fiecare dată când postezi ceva pe Facebook trimiţi mai întâi datele acelea către Facebook, iar apoi ei acordă accesul la ele anumitor utilizatori.

JULIAN: Chiar şi limita dintre guvern şi corporaţii este estompată. Dacă ar fi să ne uităm la expansiunea din sectorul antreprenorial militar în Occident în ultimii zece ani, vedem că NSA, care era cea mai mare agenţie de spionaj din lume, avea în registrele sale zece contractori principali cu care lucra. Acum doi ani avea peste 1.000. Deci se estompează graniţa dintre ceea ce reprezintă guvern şi ceea ce reprezintă sectorul privat.

JÉRÉMIE: Şi se poate susţine că agenţiile de spionaj ale SUA au acces la toate datele stocate de Google.

JULIAN: Dar chiar au.

JÉRÉMIE: Şi la toate datele Facebook, deci într-un fel Facebook şi Google ar putea fi prelungiri ale acestor agenţii.

JULIAN: Tu ai vreo somaţie Google, Jake? A primit cumva Google o somaţie pentru a preda informaţiile referitoare la contul tău Google? în cazul Wikileaks s-au trimis somaţii la Dynadot, compania din California unde se înregistrează numele de domeniu şi unde este înregistrat şi wikileaks.org. Erau somaţii care făceau parte din investigaţia secretă a Marelui Juriu împotriva Wikileaks şi în care se cereau arhivele financiare, arhivele de autentificări etc. Şi pe care Google i le-a dat.57

JACOB: *Wall Street Journal* a relatat că Twitter, Google şi Sonic, net, trei servicii pe care le folosesc sau pe care le-am folosit în trecut, au primit fiecare câte o notificare 2703 (d), tipul acesta neobişnuit de somaţie

secretă.58

JULIAN: În temeiul PATRIOT Act?

JACOB: Nu. Aici este vorba, în esenţă, de Legea Comunicaţiilor Arhivate. *Wall Street Journal* spune că fiecare dintre aceste servicii pretinde că guvernul vrea metadatele, iar guvernul a declarat că are dreptul de a face acest lucru fără mandat. Există un proces în curs de desfăşurare despre dreptul guvernului de a-şi ţine tacticile secrete, nu doar faţă de public, ci şi faţă de tribunale. Citesc *Wall Street Journal* şi am aflat şi eu ca toţi ceilalţi.

JULIAN: Deci Google s-a pus bine cu guvernul SUA în cadrul investigaţiei împotriva Wikileaks, când guvernul a emis o somaţie pentru arhivele tale – nu o somaţie normală, ci această somaţie specială, pentru spionaj. Dar apăruse ştirea, undeva la începutul lui 2011, că Twitter ar fi primit mai multe somaţii, emise de acelaşi Mare Juriu, dar Twitter s-a luptat în instanţă pentru a putea anunţa oamenii ale căror conturi erau somate – pentru a fi ridicată interdicţia de a notifica părţile vizate. Nu am un cont de Twitter, deci eu nu am primit una, dar numele meu şi cel al lui Bradley Manning erau pe toate somaţiile, figurând în dreptul informaţiei căutate. Jake, tu aveai un cont de Twitter, deci Twitter a primit o somaţie referitoare la tine. Şi Google. a primit o somaţie, dar nu s-a luptat în instanţă pentru a o face publică.59

JACOB: Aşa se pare. Aşa am citit în *Wall Street Journal*. S-ar putea să nu am nici măcar voie să fac referire la acest lucru decât în legătură cu *Wall Street Journal*.

JULIAN: cumva din cauză că aceste ordine au o clauză de păstrare forţată a tăcerii? Lucrul ăsta a fost declarat neconstituţional, nu-i aşa?

JACOB: Poate că nu. În cazul procesului Twitter, e ştiut public faptul că am pierdut moţiunea de suspendare

în care am spus că cedarea acestor date guvernului ar cauza daune ireparabile, din cauză că nu le va mai putea uita odată ce le-a primit. Ei au zis: „Ei bine, moţiunea de suspendare este respinsă, Twitter trebuie să cedeze datele”. Acum am făcut recurs în instanţă, în special în cazul ţinerii secrete a evidenţei sentinţelor – şi pot să vorbesc despre asta –, dar, după cum arată lucrurile acum, curtea a afirmat că nu te poţi aştepta la confidenţialitate pe internet, când destăinui în mod voluntar informaţii unor terţi, şi, apropo, toată lumea e o terţă persoană pe internet.

JULIAN: Chiar dacă organizaţii ca Facebook şi Twitter spun că informaţia va rămâne privată.

JACOB: Sigur. Iar aceasta este estomparea graniţelor dintre stat şi corporaţii. Poate lucrul cel mai important pe care trebuie să ni-l amintim este acesta, că NSA şi Google au un parteneriat în securitate cibernetică din raţiuni de apărare naţională.

ANDY: Orice ar însemna securitate cibernetică în acest context. E un termen foarte larg.

JACOB: Încearcă să scoată totul de sub Legea Libertăţii Informaţiei şi să ţină totul secret. Apoi, guvernul SUA afirmă de asemenea că are dreptul de a trimite somaţii administrative care au o autoritate mai mică decât un mandat de percheziţie, somaţii în cazul cărora terţii au interdicţia de a te anunţa în legătură cu ele, iar tu nu ai niciun drept de a ataca asta în instanţă, pentru că sunt implicaţi în mod direct doar terţii, iar terţii nu au niciun temei constituţional pentru a-ţi proteja datele.

JULIAN: Terţii fiind Twitter sau Facebook sau ISP[3]-ul tău.

3 „Internet Service Provider“ - Furnizor de internet (n.tr.)

JACOB: Sau oricine. Au spus că există, în cazul confidenţialităţii bancare sau al formării unui număr de telefon, o legătură directă, de tipul *one-to-one* [unul către unul]. Prin simplul fapt că folosiţi telefonul, divulgaţi numărul, de bunăvoie, companiei respective de telefonie. Ştiaţi asta, nu? Folosind telefonul spuneţi în mod evident: „Nu am nicio aşteptare de confidenţialitate” atunci când formaţi acele numere. Există o conexiune încă şi mai puţin explicită cu aparatul. Oamenii nu înţeleg cum funcţionează internetul – nu înţeleg nici cum funcţionează reţelele de telefonie dar tribunalele au hotărât de fiecare dată că aşa stau lucrurile, iar în procesul nostru Twitter de până acum, despre care din păcate nu pot vorbi pentru că nu trăiesc într-o ţară liberă, se spune, în esenţă, acelaşi lucru.60

Este nebunie curată să ne imaginăm că predăm toată informaţia personală acestor companii, iar companiile au devenit, în esenţă, o poliţie secretă privatizată. Iar – în cazul Facebook – există chiar supraveghere democratizată. În loc să fie plătiţi, cum făcea Stasi în Germania de Est, oamenii sunt recompensaţi ca cultură – acum şi-o trag. Anunţă despre prietenii lor: „Hei, cutare s-a logodit”; „A, cutare s-a despărţit”; „A, acum ştiu pe cine să sun”.

AN DY: Au fost oameni care au reuşit să facă presiuni ca Facebook să le dezvăluie toate datele arhivate despre ei, conform Legii Europene a Protecţiei Datelor, şi cantitatea cea mai mică a fost de 350 MB, cea mai mare a fost în jur de 800 MB.61 Lucrul interesant este că astfel a ieşit la iveală structura bazei de date a Facebook-ului. De fiecare dată când intri pe Facebook se înregistrează adresa ta de IP şi toate celelalte lucruri, fiecare click pe care-l faci, fiecare accesare şi numărul de accesări ale unei pagini, astfel încât să poată să-şi dea seama dacă îţi place sau nu şi aşa mai departe. Dar acest lucru a dezvăluit că

identificatorul-cheie al structurii bazei de date este cuvântul „target”. Nu-i numesc pe aceşti oameni „abonaţi” sau „utilizatori” sau mai ştiu eu cum, îi numesc „ţinte”, la care ai putea spune: „Bine, e un termen din marketing”.

JULIAN: Dar era privat pe plan intern.

ANDY: Da, dar ar putea fi ţinte şi într-un sens militar, sau ar putea fi ţinte într-un sens de spionaj. Deci ţine doar de contextul în care sunt folosite datele.

J U LI AN: Da. Asta face ca lucrul ăsta să fie atât de înspăimântător.

ANDY: Mie mi se pare foarte util lucrul ăsta. Obişnuiam să spunem, în cazul Facebook-ului, că utilizatorul nu este de fapt consumatorul. Utilizatorul Facebook este de fapt produsul, iar adevăratul consumator sunt companiile de publicitate. Este explicaţia cea mai puţin paranoică, cea mai inofensivă despre ceea ce se petrece.

Dar problema este că nu poţi învinovăţi o companie că se supune legilor unei ţări. Este normal să fie aşa, şi este o infracţiune dacă companiile nu se supun legilor ţării. Deci e destul de greu să spui că „Hei, se supun legii”. Ce fel de acuzaţie mai e şi asta?

JACOB: Nu, e un lucru cu care trebuie să fiu în dezacord în afirmaţia asta. Dacă construieşti un sistem care înregistrează totul despre o persoană şi ştii că trăieşti într-o ţară cu legi care vor obliga guvernul să predea aceste date, poate că nu ar trebui să construieşti un astfel de sistem. Iar asta este diferenţa dintre o abordare de tipul „confidenţialitate-prin-politică” şi una de tipul „confidenţialitate-prin-construcţie” în crearea unor sisteme sigure. Dacă încerci să transformi oamenii în ţinte şi ştii că trăieşti într-o ţară care face asta în mod explicit, atunci dacă Facebook şi-ar instala serverele în Libia lui Gaddafi

sau în Siria lui Assad ar fi un lucru foarte neglijent. Şi totuşi, niciuna dintre scrisorile de siguranţă naţională care au fost emise, cred, anul trecut sau acum doi ani nu aveau nimic de-a face cu terorismul. Vreo 250.000 au fost folosite pentru orice altceva, numai nu pentru a lupta împotriva terorismului.62 Deci ştiind că aceasta este realitatea, aceste companii au o răspundere etică serioasă care izvorăşte din faptul că construiesc aceste sisteme şi că au luat practic decizia economică de a-şi vinde utilizatorii. Iar ăsta nici măcar nu e un lucru tehnic. Nu are nicio legătură cu tehnologia, e vorba despre economie.

Au decis că este mai important să colaboreze cu statul şi să-şi vândă toţi utilizatorii şi să le încalce confidenţialitatea şi să facă parte dintr-un sistem al controlului – să fie plătiţi pentru că fac parte din cultura supravegherii, că fac parte din cultura controlului – decât să-i opună rezistenţă, aşa că au devenit o parte integrantă. Sunt complici şi răspunzători.

ANDY: Răspunderea etică nu e o chestiune chiar atât de importantă în zilele noastre, nu-i aşa?

Combaterea supravegherii totale cu legile fizicii

JÉRÉMIE: O întrebare care ar putea fi ridicată acum ar fi: care este soluţia, fie pentru utilizatorul individual, fie pentru societate în întregul ei? Există soluţii tehnice – servicii descentralizate, ca fiecare să-şi găzduiască propriile date, ca toată lumea să aibă încredere în furnizori apropiaţi lor, care să-i ajute cu servicii de criptare a datelor, şi aşa mai departe. Iar apoi există opţiunea diverselor politici pe care le-am discutat. Nu sunt sigur că în acest moment putem răspunde la întrebarea dacă una dintre cele două abordări este mai bună. Cred că trebuie să dezvoltăm cele două abordări în paralel. Trebuie să avem software liber, pe care să-l înţeleagă toată lumea, pe

care toată lumea să-l poată modifica şi pe care fiecare să îl poată examina pentru a fi sigur de ceea ce face. Cred că software-ul liber este una din bazele pentru o societate online liberă, pentru a avea oricând posibilitatea de a controla maşina şi de a nu lăsa maşina să te controleze pe tine. Trebuie să avem o criptografie puternică, pentru ca atunci când vrei ca datele tale să fie citite doar de tine, nimeni să nu le mai poată citi. Avem nevoie de instrumente de comunicare ca Tor sau Cryptophone, pentru a putea comunica doar cu oamenii cu care vrei să comunici. Dar se prea poate ca puterea statului şi puterea companiilor să depăşească întotdeauna puterea unor experţi în calculatoare ca noi şi capacitatea noastră de a elabora şi distribui tehnologiile astea. De asemenea, s-ar putea să avem nevoie, în timp ce vom construi tehnologiile astea, de legi şi de instrumente care să fie în mâinile cetăţenilor, pentru a putea controla ceea ce se face cu tehnologia – chiar dacă nu întotdeauna în timp real – şi pentru a-i putea sancţiona pe cei care folosesc tehnologia într-un mod neetic şi într-un mod care încalcă confidenţialitatea cetăţenilor.

JULIAN: Vreau să mă uit la ceea ce văd ca fiind o diferenţă între perspectiva cypherpunk în Statele Unite şi perspectiva europeană. Al Doilea Amendament al SUA este dreptul de a purta armă. Chiar recent am văzut o filmare, realizată de un prieten în SUA, despre dreptul de a purta armă, iar deasupra unui magazin de armament era un semn pe care scria „Democracy, Locked and Loaded” [Democraţia, încărcată şi gata să tragă]. Acesta este modul în care te asiguri că nu ai regimuri totalitare – oamenii sunt înarmaţi, iar dacă sunt destul de enervaţi îşi iau pur şi simplu armele şi preiau controlul cu forţa. O întrebare interesantă e dacă argumentul acesta mai e încă valabil,

din cauza diferenţierii tipurilor de arme care a avut loc în ultimii treizeci de ani. Ne putem aminti de afirmaţia că crearea de coduri – furnizarea de coduri criptografice secrete pe care guvernul nu le poate spiona – este în realitate o formă de muniţie. Am dus acest mare război în anii ’90 pentru a încerca să aducem criptografia la îndemâna tuturor şi l-am câştigat în mare parte.63

JACOB: În Occident.

JULIAN: Am câştigat în Occident, iar acum se află în fiecare browser, deşi poate că acum este supravegheată şi subminată în diverse moduri.64 Chestiunea este că nu poţi avea încredere că guvernul va implementa politicile pe care spune că le implementează, aşa că trebuie să asigurăm noi instrumentele de bază, instrumentele criptografice pe care le controlăm noi, ca un fel de uz de forţă, în sensul că, dacă cifrarea merge bine, guvernul nu va putea, oricât de tare ar încerca, să aibă acces la comunicaţiile noastre în mod direct.

JACOB: Puterea aproape oricărei autorităţi moderne este derivată din violenţă sau din ameninţarea cu violenţa. Trebuie să acceptăm faptul că în cazul criptografiei violenţa nu va putea rezolva niciodată o problemă de matematică.

JULIAN: Exact.

JACOB: Acesta este lucrul important. Nu înseamnă că nu poţi fi torturat, nu înseamnă că nu vor putea să-ţi instaleze microfoane în casă sau să o submineze în vreun fel, dar înseamnă că dacă găsesc un mesaj criptat nu contează dacă au forţa autorităţii în spatele oricărei acţiuni pe care o fac, tot nu vor putea rezolva acea problemă de matematică. Acesta însă este un lucru care nu este evident pentru oamenii care nu sunt tehnici, şi trebuie să facem în aşa fel încât să devină evident. Dacă am putea

rezolva acele probleme de matematică ar fi o altă poveste şi, sigur, dacă cineva ar fi în stare să le rezolve, guvernul ar fi acela.

JULIAN: Dar se întâmplă ca o caracteristică a realităţii în care trăim, la fel precum cea reprezentată de faptul că poţi construi bombe atomice, să fie aceea că există unele probleme matematice care pot fi elaborate şi pe care nici cel mai puternic stat nu le poate rezolva. Cred că lucrul acesta a fost foarte atrăgător pentru libertarii din California, şi nu numai, care au crezut în idealul acesta al „democraţiei încărcate şi gata să tragă”, pentru că aveau aici un mod foarte intelectual de a o face – câţiva indivizi ţinând piept întregii forţe a celei mai puternice puteri din lume prin intermediul criptografiei.

Aşadar exista o proprietate a universului care se află de partea confidenţialităţii, fiindcă unii algoritmi de criptare nu pot fi sparţi de niciun guvern, niciodată. Mai sunt alţii despre care ştim că sunt extrem de greu de spart, chiar şi pentru NSA. Ştim aceasta pentru că chiar ei recomandă antreprenorilor armatei SUA să folosească aceşti algoritmi pentru protejarea comunicaţiilor strict secrete ale armatei, iar dacă ar exista vreo modalitate de a-i sparge ar fi fost găsită repede de ruşi sau de chinezi, cu consecinţe grave pentru cel care a luat decizia de a recomanda un cifru nesecurizat. Deci cifrurile sunt acum destul de bune, avem destulă încredere în ele. Din păcate nu poţi avea deloc încredere în aparatul cu care le foloseşti, deci asta este o problemă. Dar lucrul ăsta nu duce la interceptare în masă; duce la urmărirea computerelor unor anumiţi oameni. Este foarte greu să securizezi un computer dacă nu eşti un expert în securizare. Dar criptografia poate rezolva problema interceptării în masă, iar problema interceptării în masă

este cea care pune în pericol civilizaţia globală. Nu urmărirea individuală este ameninţarea.

Cu toate acestea, sunt de părere că avem de-a face cu forţe economice şi politice uriaşe, după cum a spus şi Jérémie, iar rezultatul cel mai probabil este că eficienţa naturală a tehnologiilor de supraveghere comparată cu numărul oamenilor va duce la faptul că încetul cu încetul vom deveni o societate poliţienească totalitară şi globală – prin totalitară vreau să spun una a supravegherii totale – şi că probabil ultimii oameni liberi rămaşi în viaţă vor fi cei care înţeleg cum să folosească criptografia pentru a se apăra împotriva acestei supraveghei complete, totale, precum şi unii oameni care au ieşit complet din sistem, neoluddiţi care s-au ascuns în peşteri sau popoare tribale tradiţionale care nu au niciunul din avantajele unei economii moderne, deci capacitatea lor de a juca vreun rol este foarte limitată. E evident că oricine poate să stea departe de internet, dar atunci le este foarte dificil să aibă vreo influenţă. Făcând lucrul acesta îşi elimină posibilitatea de a fi influenţi. Este aceeaşi situaţie cu telefoanele mobile; poţi alege să nu ai un telefon mobil, dar îţi reduci influenţa. Nu e o cale înainte.

JÉRÉMIE: Dacă priveşti lucrurile dintr-o perspectivă de piaţă, sunt convins că există o piaţă a confidenţialităţii care a rămas în mare parte neexplorată, aşa că poate va exista un stimulent economic pentru unele companii de a crea instrumente care le vor acorda utilizatorilor posibilitatea individuală de a-şi controla datele şi comunicaţiile. Poate că aceasta este o modalitate în care putem rezolva această problemă. Nu sunt sigur dacă ar putea funcţiona de una singură, dar aceasta s-ar putea întâmpla şi s-ar putea să nu o ştim încă.

JULIAN: Criptografia va fi peste tot. Este lansată de

toate marile organizaţii, care tind să se transforme într-o reţea de oraşe-stat. Dacă e să ne gândim la căile de comunicare de pe internet – tranzacţii financiare transnaţionale rapide, organizaţii transnaţionale, interconexiuni între subdiviziuni ale organizaţiilor –, toate acele fluxuri de informaţii trec prin canale de comunicaţie nesecurizate. Este asemenea unui organism fără piele. Există organizaţii şi state care ajung să nu se mai distingă unele de altele – fiecare reţea de influenţă mondială concurând pentru avantaj –, iar comunicaţiile lor sunt expuse oportuniştilor, concurenţilor statelor şi aşa mai departe. Aşa că se construiesc reţele noi, peste internet, reţele virtuale private, iar confidenţialitatea lor e garantată de criptografie. Aceasta este o bază a puterii industriale care împiedică interzicerea criptografiei.

Dacă ar fi să ne uităm la telefonul Blackberry, de exemplu, acesta are un sistem de criptare inclus care poate fi folosit în interiorul reţelei Blackberry. Research în Motion, compania canadiană care-l operează, poate descifra traficul utilizatorilor şi are centre de date cel puţin în Canada şi în Regatul Unit, iar în acest fel alianţa anglo-americană a spionajului poate avea acces la comunicaţiile Blackberry către Blackberry din lumea întreagă. Dar companiile mari folosesc acest principiu în moduri mai sigure. Guvernele occidentale au fost de acord cu lucrul acesta până în momentul în care s-a extins de la corporaţii la indivizi, iar apoi am văzut exact aceleaşi reacţii politice ostile pe care le-am văzut în Egipt, sub guvernul lui Mubarak.65

Cred că singura apărare eficientă împotriva distopiei supravegherii care se apropie este cea în care iei singur măsuri pentru a-ţi proteja confidenţialitatea, deoarece oamenii care au capacitatea de a intercepta totul nu au

nicio motivaţie pentru a-şi limita acţiunile. O analogie istorică ar putea-o reprezenta felul în care au învăţat oamenii că ar trebui să se spele pe mâini. A fost nevoie de formularea teoriei microbilor şi de popularizarea ei şi de instalarea paranoiei despre răspândirea bolilor prin nişte chestii invizibile de pe mâini, pe care nu le puteai vedea aşa cum nu poţi vedea interceptarea în masă. Odată ce a fost înţeles fenomenul, producătorii de săpun au creat produse pe care oamenii le-au consumat pentru a-şi calma frica. Este necesar ca frica să pună stăpânire pe oameni astfel încât aceştia să înţeleagă problema şi abia apoi se va crea destulă cerere pentru ca ea să fie rezolvată.

Există o problemă şi de partea opusă a ecuaţiei, şi anume faptul că programele care pretind că sunt securizate, care pretind că conţin criptografie sunt deseori escrocherii, din cauză că criptografia este complexă, iar escrocheria poate fi ascunsă în complexitate.66

Deci oamenii vor trebui să se gândească la acest lucru. Singura întrebare este în care dintre cele două feluri se vor gândi la el. Fie se vor gândi că „Trebuie să fiu atent la ce spun, trebuie să mă conformez" tot timpul, în fiecare interacţiune, fie se vor gândi că „Trebuie să-mi însuşesc mici componente ale acestei tehnologii şi să-mi instalez lucruri care să mă protejeze astfel încât să-mi pot exprima liber gândurile şi să comunic liber cu prietenii mei şi cu oamenii la care ţin". Dacă oamenii nu adoptă modalitatea a doua, vom avea o corectitudine politică universală, pentru că oamenii se vor autocenzura chiar şi atunci când vor vorbi cu prietenii lor cei mai apropiaţi şi se vor elimina din postura de actori politici.

Internetul şi politica

JÉRÉMIE: Este interesant să observi puterea hackerilor – „hacker" în sensul primar al cuvântului, nu în

cel de infractor. Hackerul este un iubitor al tehnologiei, cineva căruia îi place să înţeleagă cum funcţionează tehnologia, nu pentru a fi captivul tehnologiei, ci pentru a o face să funcţioneze mai bine. Bănuiesc că la vârsta de cinci sau şapte ani aţi avut şi voi şurubelniţă şi aţi încercat să deschideţi un aparat pentru a vedea cum este pe dinăuntru. Asta înseamnă să fii un hacker, iar hackerii au construit internetul din mai multe motive, inclusiv pentru că era o distracţie, şi l-au dezvoltat şi au dat internetul tuturor. Companii ca Google sau Facebook au văzut oportunitatea de a-şi construi modele de afaceri bazate pe preluarea datelor personale ale utilizatorilor. Dar totuşi putem observa o formă de putere în mâinile hackerilor. Ceea ce mă interesează în principal în ultima vreme este faptul că aceşti hackeri capătă putere, chiar şi în arenele politice. În SUA s-a propus această legislaţie SOPA (Legea Opririi Pirateriei Online) şi PIPA (Legea pentru Protecţia IP-urilor) – reglementări violente ale drepturilor de autor care, în esenţă, acordă Hollywoodului puterea de a ordona oricărei companii de internet să restricţioneze accesul şi să cenzureze internetul.67

JULIAN: Şi blocade financiare asemenea celei la care este supusă Wikileaks.68

JÉRÉMIE: Exact. Ceea ce s-a întâmplat în cazul Wikileaks din cauza companiilor bancare devenise metoda standard pentru a lupta cu piraţii ticăloşi ai drepturilor de autor care au omorât Hollywoodul şi aşa mai departe. Şi am fost martorii acestui tumult uriaş creat pe internet de societatea civilă – şi nu doar în Statele Unite, fenomenul nu ar fi funcţionat dacă doar cetăţenii SUA s-ar fi ridicat împotriva SOPA şi PIPA. Au participat oameni din toată lumea, iar hackerii s-au aflat în centrul lucrurilor şi au furnizat celorlalţi instrumente pentru a înlesni participarea

în dezbaterea publică.

JULIAN: Pentru a ajuta la construirea campaniei.

JÉRÉMIE: Nu cumva pe Tumbir, sau pe un alt site de genul ăsta, poţi să-ţi laşi pe prima pagină numărul de telefon, urmând apoi să fii sunat şi pus în legătură cu Congresul? Şi puteai pur şi simplu să începi să vorbeşti cu cineva şi să spui „Da, ce faceţi voi e o tâmpenie”.

JACOB: Internetul a fost folosit pentru autoapărare.

JÉRÉMIE: Eu cred că noi, ca hackeri, avem o răspundere faţă de instrumentele pe care le construim şi pe care le distribuim restului lumii, şi putem fi martorii începutului eficienţei cu care această răspundere poate fi pusă în practică când o folosim colectiv. Astăzi, Uniunea Europeană se află în procesul dezbaterii ACTA – ACTA (Acordul Comercial de Combatere a Contrafacerii) este un tratat multinaţional care stă la baza legilor SOPA şi PIPA.69 Tocmai m-am întors de la Parlamentul European unde noi, ca indivizi, indivizi bărboşi şi mirositori, am dictat unei comisii parlamentare. Le-am arătat articole în regulile de procedură ale

Parlamentului European pe care păreau că le văd pentru prima oară şi le-am spus cum să procedeze şi am câştigat votul cu 21 la 5, lucru care a marginalizat raportorul britanic într-un colţ îndepărtat. Aceasta este o parte foarte mică dintr-o mică chestiune procedurală pe calea spre înfrângerea acordului ACTA, acest acord global monstruos care a fost creat în secret pentru a circumscrie democraţia însăşi. Dar ar fi posibil să omorâm acest monstru, în calitate de cetăţeni – uşor, cu instrumentele internetului, cu listele de e-mailuri, cu wiki-urile, cu platformele de chat ale IRC[4] etc. –, şi cred că putem fi

4 Internet Relay Chat - comunicare instantanee pe internet (n.tr.)

martorii trecerii internetului de la copilărie la adolescenţă şi ai felului în care poate fi el folosit de societatea întreagă pentru a încerca să facă lucrurile să se schimbe. Cred că este de o importanţă uriaşă faptul că noi, hackerii, suntem aici cu cunoştinţele noastre tehnice pentru a ghida oamenii şi pentru a le spune: „Ar trebui să folosiţi această tehnologie care vă permite controlul asupra confidenţialităţii datelor voastre, în loc de Facebook sau Google”, şi că cele două se articulează împreună destul de bine – sau ar putea să se articuleze împreună destul de bine. Este un pic de optimism aici.

JULIAN: Jake, vorbind despre această radicalizare politică a tineretului de pe internet, tu ai călătorit în toată lumea, mai cu seamă în ultimii doi ani, vorbind despre Tor, vorbind cu oameni care vor anonimitate, care vor confidenţialitate faţă de propriul guvern, şi trebuie să fi văzut acest fenomen în ţări diferite. Este un lucru semnificativ?

JACOB: Cu siguranţă. Exemplul canonic la care mă gândesc imediat este vizita în Tunisia. Am fost în Tunisia după căderea regimului lui Ben Ali şi am vorbit despre Tor la un curs de informatică la care au participat şi nişte oameni foarte tehnici de la universitate, iar cineva a ridicat mâna şi a spus:» Dar cum rămâne cu oamenii ticăloşi?” Iar apoi a trăncănit întruna despre cei Patru Călăreţi ai Apocalipsei Informatice – spălarea de bani, drogurile, terorismul şi pornografia infantilă.» Cum rămâne cu oamenii ticăloşi?” Aceste patru lucruri sunt aduse tot timpul în discuţie şi spectrul lor este folosit pentru a ataca tehnologiile de apărare a confidenţialităţii, pentru că e evident că trebuie să eliminăm aceste patru grupuri. Aşa că i-am întrebat pe cei aflaţi la curs: „Cine a văzut vreodată pagina Ammar 404?”, care este pagina de

cenzură introdusă de regimul Ben Ali înainte şi în timpul revoluţiei, pentru a bloca accesul. Fiecare persoană din clasă a ridicat mâna, inclusiv profesorul, în afară de cea care pusese întrebarea. Şi m-am uitat la fata care pusese această întrebare şi i-am zis: „Priveşte la toţi oamenii din jurul tău. Adică la toţi colegii tăi. Crezi tu cu adevărat că a meritat ca toate persoanele din clasă să fie asuprite pentru a lupta împotriva acelor lucruri?” Şi a zis: „De fapt, am să ridii: şi eu mâna”.

S-a vorbit ceva mai mult de atât, dar în esenţă oamenii care văd lucrurile în context îşi dau seama care este situaţia reală. Asta schimbă situaţia în mod dramatic. Iar asta se întâmplă în toată lumea, tot timpul – dar de obicei se întâmplă mai târziu, adică oamenii se uită înapoi şi îşi dau seama că ar fi putut folosi acea tehnologie, îşi dau seama că „A, da, se pare că nu e vorba doar de ticăloşi pentru că, de fapt, eu sunt ticălosul dacă încerc să vorbesc în mod liber despre ceva, iar cuiva de la putere nu-i place ce am de spus despre asta”. Şi poţi observa că are loc o deşteptare.

Dar e fals să spui că s-a întâmplat doar în ultimii doi ani. Îmi pare rău să-ţi fac asta, Julian, dar tu eşti o parte a radicalizării generaţiei mele. Eu sunt un cypherpunk de generaţia a treia, dacă am număra aşa. Munca pe care aţi depus-o tu şi Ralf Weinmann la sistemul de fişiere *rubberhose* a fost, în parte, cea care m-a inspirat pe mine să lucrez la sisteme de criptare. Sistemul criptografic de fişiere pe care l-am creat, numit M.A.I.D, a fost o reacţie la lucruri cum ar fi legea *Régulation of Investigatory Powers* [Reglementarea Puterilor Investigatoare] din Regatul Unit, prin care, în esenţă, statul a decis că soluţia la criptografie este reglementarea negativă şi că îţi poate fi luată parola.70 Desigur, în cazul lui Julian, când au creat asta a

fost din cauză că regimurile opresive torturau oamenii pentru o parolă, deci trebuia să poţi da mai multe parole pentru a face faţă torturii lor. Sistemul meu criptografic, M.A.I.D., a fost creat pentru un sistem legal în care acuzatul are dreptul de a păstra tăcerea, dar poate dovedi, dacă este constrâns, că spune adevărul, fără a încălca confidenţialitatea. Când am văzut activitatea lui Julian mi-am dat seama că poţi folosi tehnologia pentru a da oamenilor obişnuiţi puterea de a schimba lumea. Întorcându-mă înapoi la vechea listă de e-mailuri Cypherpunk cu Tim May, unul dintre membrii ei fondatori, şi citind vechile postări ale lui Julian în lista Cypherpunk, realizez că asta e ceea ce a determinat o întreagă generaţie de oameni să devină mai radicali, pentru că oamenii şi-au dat seama că nu mai erau atomizaţi, că puteau petrece ceva timp scriind un software care ar putea duce la emanciparea a milioane de oameni.71

Există însă nişte consecinţe neintenţionate ale dezvoltării acestui lucru, pentru că cei care au creat Google nu şi-au propus să creeze Google, să creeze cea mai mare maşinărie de supraveghere care a existat vreodată. Dar de fapt asta s-a creat, iar de îndată ce oamenii vor începe să-şi dea seama de acest lucru, vor începe să trimită acele Scrisori de Siguranţă Naţională, nu?

JÉRÉMIE: Cred că sunt trei lucruri de importanţă crucială în ceea ce ai spus.

JACOB: Doar trei?

JÉRÉMIE: Printre altele.

ANDY: Ok, lăsaţi-mă să-l adaug pe cel de-al patrulea, bine?

JACOB: Dar încă nici nu ştii care sunt acelea trei.

JÉRÉMIE: Văd trei elemente-cheie legate între ele.

Nu spun că ele ar trebui luate separat, dar unul dintre ele îl reprezintă regimurile autoritare şi puterile pe care le au regimurile autoritare într-o epocă a tehnologiilor digitale. În cazul regimului lui Ben Ali – iar astăzi lucrul acesta este evident în foarte multe alte regimuri –, poţi decide ce anume pot să afle oamenii sau cu cine pot comunica. Lucrul acesta presupune o putere enormă şi ar trebui să ne împotrivim lui, iar internetul – un internet liber – este un instrument prin care să ne împotrivim lucrului acestuia. Un alt element-cheie este construcţia unor instrumente şi tehnologii mai bune, tehnologii care pot încerca să ocolească probleme precum cenzura, dar, în mare, instrumente care să facă parte din infrastructura care să ne ajute să răsturnăm dictatorii. Iar încă o problemă este discursul politic pe care l-ai evocat, cei Patru Călăreţi ai Apocalipsei Informatice, pretextele care sunt folosite în fiecare zi de către politicieni în mass-media – „Vom muri cu toţii din cauza terorismului? Avem nevoie de Patriot Act”; „Cei care distribuie pornografie infantilă sunt peste tot”; „Internetul este plin de pedo-nazişti, deci e nevoie de cenzură”.

JACOB: Pedo-nazişti?

JÉRÉMIE: Pedo-nazişti, da – pedo-nazi.com e rezervat deja. „Artiştii vor muri de foame şi nu va mai exista cinema, aşa că trebuie să dăm Hollywoodului puterea de a cenzura internetul”, şi aşa mai departe. Cred că şi în acest caz internetul este un instrument, un antidot împotriva discursului politic. Discursul politic se bazează pe sentimentalism şi pe un cadru temporal al prezentării informaţiei extrem de scurt – informaţia apare şi dispare după douăzeci şi patru de ore şi este înlocuită de informaţie nouă. Cu ajutorul internetului, am senzaţia că suntem în procesul de a construi ceea ce eu numesc timpul

internetului. Din cauză că marele internet nu uită niciodată, putem construi dosare pe parcursul anilor, în fiecare zi, şi putem elabora, putem analiza. Asta e ceea ce am făcut în ultimii trei ani cu ACTA. Şi, din nou, Wikileaks iie-a inspirat, fiindcă prima versiune a ACTA care a fost scursă a fost scursă la Wikileaks în 2008.72

JULIAN: Da, am cules-o noi.

JÉRÉMIE: Şi am scurs şi noi două versiuni. În ultimii trei ani au existat cinci versiuni ale textului pe care le-am putut lua şi spune, paragraf cu paragraf, rând cu rând, că cutare face lucrul ăsta, aici e industria care cere cutare lucru, şi am putut să implicăm experţi legali şi experţi tehnologici şi să construim un discurs politic diferit de oficialul „Avem nevoie de ACTA pentru a salva cultura şi a salva copiii de medicamentele false" şi alte afirmaţii de genul ăsta. Aşa că ne-am construit propriul program politic mulţumită timpului internetului, prin analiză precisă, muncă grea, conectând oamenii unii cu alţii pentru a participa la lucrul acesta.

JULIAN: E adevărat, şi cred că viziunea aceasta asupra ACTA a cucerit publicul.

JÉRÉMIE: Până acum e bine.

JULIAN: Aceasta cred că va fi viziunea istorică, dar, în spatele cortinei, acest aşa-numit Acord Comercial de Combatere a Contrafacerii, care a fost propus de industria drepturilor de autor a SUA, a fost de fapt folosit într-o mulţime de tratate bilaterale, pentru a încerca să se creeze un nou regim internaţional privitor la ce este legal şi ce nu este legal în ceea ce priveşte publicarea şi la mecanismele care pot fi folosite pentru a împiedica oamenii de la publicarea anumitor lucruri. Standardizează o versiune mai dură a legii DINCA din Statele Unite (Legea privind Drepturile de Autor Digitale), care spune că dacă trimiţi

cuiva o scrisoare prin care îi ceri să dea jos un lucru de pe internet, e obligat să-l dea jos, şi există un fel de proces de două săptămâni în care poate veni cu contraargumente şi aşa mai departe, dar din cauză că e scump pentru orice ISP să aibă de-a face cu contraargumente, îl coboară imediat, şi-i permit autorului sau celui care l-a urcat să se lupte singur. Efectul acestui lucru a fost destul de pronunţat în Statele Unite, în ceea ce priveşte ştergerea unei cantităţi mari de conţinut. Scientologia a abuzat de aceasta pentru a scoate efectiv mii de înregistrări video de pe YouTube.73

Deci hai să presupunem că ACTA a fost respinsă în Parlamentul European, şi chiar cu succes, cel puţin versiunea aceasta. Dar manifestările principale ale ACTA par să se petreacă oricum – a existat dezbaterea democratică, ACTA a fost demonizată în sfera publică, am ieşit învingători în discursul politic, dar în spatele cortinei au fost elaborate tratate bilaterale secrete care obţin acelaşi rezultat, tot ce au făcut a fost să submineze procesul democratic. De exemplu, Wikileaks a intrat în posesia noului acord de comerţ liber între UE şi India şi l-a publicat, acord care include bucăţi mari din ACTA.74 Acest lucru s-a întâmplat cu mai multe alte acorduri şi legislaţii. Capul ACTA ar putea foarte bine să fie tăiat, dar corpul se va despica în câteva bucăţi, iar fiecare dintre ele îşi va croi drum către alte lucruri, către ordinea internaţională sub forma acestor tratate internaţionale. Deci puteţi avea victoriile democratice care au loc în public, la suprafaţă, dar dedesubt lucrurile se fac oricum. Lucru care cred că arată că nu reforma politică sau legislativă este răspunsul; deşi nici nu poţi da adversarului o lovitură liberă, pentru că atunci va urgenta lucrurile. Deci e important să controlăm fenomenul în diverse moduri, la fel cum

controlatăm ACTA. îi încetinim manifestarea. Dar nici măcar o victorie în parlament în ceea ce priveşte legislaţia nu opreşte această activitate care se desfăşoară în strat mai profund.

JACOB: Un lucru care cred că trebuie subliniat este faptul că Roger Dingledine, unul dintre creatorii Tor, despre care aş spune că mi-e un fel de mentor şi care mi-a dat mult de gândit în ceea ce priveşte împiedicarea cenzurii şi anonimitatea online, vorbeşte despre cum, de exemplu, un firewall nu are succes doar din punct de vedere tehnic – şi este important să înţelegi tehnologia din spatele său dacă vrei să construieşti o tehnologie care să i se opună –, dar are succes şi din punct de vedere social. Oamenii care luptă împotriva acordului ACTA folosesc tehnologie, iar tehnologia le permite să stea pe poziţii, dar în realitate cea pe care este important să o înţelegem în cazul acesta este forţa reprezentată de oamenii obişnuiţi, iar vorbăria tehnică nu este lucrul important. Ceea ce contează este ca oamenii să se implice în toată povestea asta şi s-o schimbe cât încă au puterea să o facă, aşa că aspectul uman este, de fapt, partea cea mai importantă. Wikileaks a publicat documente care permit aceasta, iar distribuirea de informaţie este importantă, dar şi persoanele care preiau acea informaţie importantă şi o transmit contează. Pentru că există cel puţin argumentul că mulţi dintre noi trăim într-o democraţie, că suntem liberi, că ar trebui să fie aşa încât să fim guvernaţi prin consimţământ. Şi astfel, dacă toată lumea înţelege ce se petrece şi dacă găsim ca ceea ce se petrece nu este un lucru consimţit de noi, atunci este foarte greu să se continue şi să se treacă legile şi să se facă totul fără consimţământul celor guvernaţi.

JÉRÉMIE: Este vorba despre creşterea costurilor

politice ale luării unor decizii proaste pentru cei care le iau, şi putem face acest lucru în mod colectiv, cu un internet liber, atâta vreme cât îl avem la îndemână.

JACOB: Dar ai putea să o faci şi fără internet, pentru că am avut – în istorie – societăţi libere înainte de internet, doar că era mai costisitor din punct de vedere economic, era mai dificil în anumite privinţe, iar ăsta este motivul pentru care mişcarea peerto-peer este atât de importantă.75

ANDY: Punctul numărul patru este, cred eu, acela că arhitectura descentralizată a sistemelor este un lucru fundamental, care trebuie pus de asemenea în mâinile poporului, pentru că acum există acest cloud computing centralizat.76

JULIAN: Facebook este complet centralizat. Twitter este complet centralizat. Google este complet centralizat. Toate în Statele Unite; toate sub controlul celor care controlează forţa coercitivă. La fel ca procesul de cenzură care a început după ce Wikileaks a publicat Cablegate, când Amazon ne-a scos site-ul de pe serverele lor.77

ANDY: Iar cloud computing stimulează din punct de vedere economic companiile să aibă o modalitate mai ieftină de a procesa datele în aşa-numitele centre de date, conduse de corporaţii americane, lucru care înseamnă că aduc datele în jurisdicţia SUA, la fel ca în cazul companiilor de plăţi şi aşa mai departe.

JULIAN: Există o tendinţă în contextul trecerii la cloud computing care este destul de îngrijorătoare. Există îngrămădiri de servere într-un singur loc, pentru că este mai eficient să standardizezi astfel controlul asupra mediului înconjurător, să standardizezi sistemul de plată. Este o tehnică competitivă din cauză că acumularea de servere într-un singur loc e mai ieftină decât răspândirea

lor. Majoritatea comunicaţiei care se face pe internet, în afară de streamingul de video, se face între server şi server, deci dacă pui serverele mai aproape unul de celălalt este mai ieftin. Rezultatul îl reprezintă aceste mari stupuri de servere comunicante. Are sens ca Google, de exemplu, să-şi plaseze serverele lângă marii furnizori de conţinut, sau invers, pentru că paginile sunt indexate de Google pentru a putea fi căutate. Deci există în SUA clădiri uriaşe care sunt pur şi simplu pline de servere de la diverse companii. Astea sunt locurile în care NSA îşi instalează unele dintre punctele de colectare a interceptărilor în masă. Internetul nu ar putea exista fără această centralizare, nu din cauză că este imposibil din punct de vedere tehnologic, ci doar din cauză că este pur şi simplu mult mai eficient să fie centralizat. În competiţia economică, versiunea centralizată câştigă.

ANDY: Deşi e foarte important să înţelegem punctul de vedere arhitectural – infrastructurile centralizate fac să fie foarte uşoare controlul central şi abuzul de putere –, e de asemenea ca şi cum ai distruge micul supermarket de la colţ printr-un concept centralizat de comerţ cu amănuntul.

JULIAN: Mergându-se către o multinaţională uriaşă, cum este Safeway.

ANDY: Da, la fel cum s-a întâmplat cu shoppingul. Este foarte important să păstrăm o abordare descentralizată a infrastructurii. Când eram membru al ICANN – Internet Corporation for Assigned Names and Numbers [Corporaţia Internet pentru Alocare de Nume şi Numere], care creează şi reglementează numele de domenii de pe internet, am aflat ceva de la Vince Cerf, cel care a inventat, cel puţin în parte, protocolul TCP/IP, protocolul fundamental de comunicaţie pe internet. Avea obiceiul să spună: „Ştii, un lucru bun despre guverne e că

nu sunt niciodată singulare, sunt întotdeauna la plural”. Deci, chiar şi printre guverne, există acelea care vor să aibă propria rază de acţiune descentralizată, şi chiar în interiorul guvernelor există diferite facţiuni care se luptă între ele. Acesta este lucrul care ne va salva în final de Big

Brother, pentru că vor fi prea mulţi care vor dori să fie Big Brother şi se vor lupta între ei.

JULIAN: Nu cred, Andy. Cred că au existat la un moment dat elite naţionale care concurau una cu cealaltă, şi că acum acestea se asociază unele cu altele şi se despart de propriul popor.

ANDY: Se asociază, în sensul ăsta ai dreptate – şi nu sunt nici eu atât de sigur că ne va salva lucrul ăsta –, dar există o şansă să ne păstrăm identitatea. Trebuie să rămânem fideli propriei noastre infrastructuri, acesta este lucrul important de învăţat aici – că dacă vrem să ne opunem statului poliţienesc, unui unic Big Brother, trebuie să învăţăm ce înseamnă lucrul ăsta, dacă este într-adevăr o asociere de state centrale care îşi spun: „Hei, dacă ne unim am putea câştiga şi mai mult”. Şi trebuie să ştim care ne este rolul aici – rolul nostru este să rămânem descentralizaţi, să avem propria noastră infrastructură, să nu ne bazăm pe cloud computing şi alte tâmpenii, ci să avem sistemul propriu.

JULIAN: Dar s-ar putea să avem această dominaţie a tehnicii. Dacă este adevărat că e mai uşor să foloseşti Twitter decât să-ţi creezi propriul Twitter; dacă este adevărat că e mai uşor să foloseşti Facebook decât DIASPORA sau vreo altă alternativă; dacă este adevărat că cloud computing e mai ieftin, atunci aceste tehnici şi servicii vor fi dominante.78 Nu e vorba despre a spune că trebuie să ne creăm propriile servicii locale, pentru că aceste servicii locale nu vor putea fi competitive, pur şi

simplu, şi vor fi folosite doar de o minoritate mică de oameni. Avem nevoie de ceva mai bun decât a spune că trebuie să avem o variantă pentru săraci a Facebook-ului şi să ne aşteptăm ca oamenii să o folosească.

ANDY: Păi, revenind la Biserica Romano-Catolică, ne întoarcem la timpurile în care există un singur editor principal de carte, din cauză că Amazon caută să controleze întreg lanţul de furnizare de cărţi electronice, deci trebuie să ne păstrăm capacitatea proprie de tipărire şi publicare. S-ar putea să pară puţin exagerat, dar am văzut ce pot face aceste companii dacă nu vorj fie ele, fie agenţiile guvernamentale de care depind în jurisdicţia lor, ca unele lucruri să se întâmple. Şi cred că pasul următor va trebui să fie, evident, că vom avea nevoie de propriii noştri bani, astfel încât, chiar dacă nu le place că susţinem proiecte ca Wikileaks sau mai ştiu eu ce, noi vom avea modul nostru propriu de a o face, fără să ne bazăm pe o infrastructură centrală care aparţine unei singure jurisdicţii.

JÉRÉMIE: Aş vrea să fiu de acord cu ceea ce spune Andy. Cred că arhitectura contează şi că acest lucru este crucial pentru tot ceea ce susţinem. Dar acesta este un mesaj pe care avem răspunderea de a-l comunica publicului, pentru că noi îl înţelegem, ca hackeri, ca tehnicieni care construiesc internetul zilnic şi se joacă cu el. Şi poate că aceasta este o modalitate de a câştiga inimile şi minţile tinerelor generaţii. Din cauza asta cred că războaiele drepturilor de autor sunt esenţiale, pentru că, prin intermediul tehnologiilor de tipul peer-to-peer, de când cu Napster în 1999, oamenii au înţeles – au prins ideea – că distribuind fişiere între indivizi…

JULIAN: Eşti un infractor.

JÉRÉMIE: Nu, construieşti o cultură mai bună.

JULIAN: Nu, eşti un infractor.

JÉRÉMIE: Ăsta e discursul, dar dacă construieşti o cultură mai bună pentru tine însuţi, toată lumea va folosi Napster.79

ANDY: Istoria rasei umane şi istoria culturii sunt istoria copierii gândurilor, a modificării lor şi a procesării lor ulterioare, şi dacă numeşti asta furt, eşti la fel ca toţi cinicii.

JÉRÉMIE: Exact, exact! Cultura e făcută pentru a fi distribuită.

JULIAN: Păi începând cu anii ’50, în Occident am avut o cultură industrială. Cultura noastră a devenit un produs industrial.

JÉRÉMIE: Cred că ce facem noi aici e să îi dăm apă la moară, fiindcă joacă rolul de avocat al diavolului şi o face foarte bine.

JACOB: Eu nu muşc momeala. E evident că e o tâmpenie.

JÉRÉMIE: Este o tâmpenie. În discursul politic se numeşte furt, dar vreau să spun că toată lumea care a folosit Napster în 1999 a devenit un fan al muzicii şi s-a dus la concerte şi a spus tuturor „Trebuie să-i asculţi pe oamenii ăştia, trebuie să te duci la concertul cutare” şi aşa mai departe. Deci oamenii au avut un exemplu practic despre cum tehnologia peer-to-peer a descentralizat arhitectura. De fapt, Napster era puţin centralizat pe vremea aceea, dar a însămânţat ideea unei arhitecturi descentralizate. Toată lumea avea un exemplu concret despre cum arhitectura descentralizată aduce un bine societăţii, iar când este vorba despre distribuirea culturii este la fel ca atunci când este vorba despre distribuirea cunoaşterii. Distribuirea cunoaşterii este lucrul despre care vorbim atunci când discutăm despre a ocoli cenzura

sau despre a ne croi drum prin discursul politic pentru a construi un sistem democratic mai bun şi pentru a îmbunătăţi societatea.

Aşadar, avem exemple în care serviciile descentralizate şi distribuţia între indivizi fac ca lucrurile să fie mai bune, iar contraexemplul este avocatul diavolului pe care-l joacă Julian, când vine o industrie şi spune: „Oh, lucrul ăsta este furt şi omoară pe toată lumea, omoară actorii, omoară Hollywoodul, omoară cinematografia, omoară pisicuţe şi totul”. Au câştigat bătălii în trecut, iar acum s-ar putea să câştigăm noi bătălia ACTA. Şi trebuie să fiu în dezacord din nou cu avocatul diavolului pe care l-a jucat

Julian înainte. ACTA a fost cel mai bun exemplu de ocolire a democraţiei de până acum, în care s-a cântat în strună parlamentului şi instituţiilor internaţionale, s-a cântat în strună opiniei publice, iar pe uşa din dos s-au impus măsuri inacceptabile. Dacă reuşim să respingem asta, atunci vom stabili un precedent, vom avea oportunitatea să impunem o agendă de lucru pozitivă, să spunem „ACTA s-a terminat, acum hai să facem ceva care e cu adevărat în favoarea publicului”. Şi lucrăm în direcţia asta, iar unii membri ai Parlamentului European înţeleg acum că atunci când indivizii distribuie lucruri, când distribuie fişiere fără profit, nu ar trebui să meargă la închisoare, nu ar trebui pedepsiţi. Cred că dacă reuşim să facem asta avem şanse bune să arătăm restului lumii că distribuirea cunoaşterii, distribuirea informaţiei fac ca lucrurile să fie mai bune, că trebuie să promovăm lucrul ăsta, şi nu să-l atacăm şi că orice încercare – fie ea legislativă sau din partea unui dictator sau a unei companii – de a lovi în capacitatea noastră de a distribui informaţii şi a distribui cunoaştere într-o manieră descentralizată

trebuie atacată. Punct. Cred că putem face ca această atitudine să ia avânt.

JULIAN: Cum rămâne cu dezbaterea PIPA/SOPA în Statele Unite? Aceasta este o legislaţie nouă, propusă în Congres pentru ca industriile SUA să creeze embargouri financiare şi blocade ale internetului în numele industriilor americane.

JACOB: A fost creată anume pentru a ataca Wikileaks şi lucruri care ţin de Wikileaks sau asemănătoare cu Wikileaks.

JULIAN: Blocada bancară împotriva noastră a fost menţionată anume în Congres ca un instrument eficace.80

J EREMIE: Şi era vorba să se dea acest instrument Hollywoodului.

JULIAN: Aşa că am organizat o mare campanie comunitară împotriva acestui lucru şi într-un final Google şi Wikipedia şi mulţi alţii s-au alăturat campaniei. Dar nu mi-am spus: „Ok, e foarte bine, am câştigat bătălia”. M-am speriat de moarte, din cauză că Google s-a văzut dintr-odată ca jucător politic, şi nu doar ca distribuitor, şi a simţit acea putere uriaşă, fantastică asupra Congresului.

JÉRÉMIE: Google era doar o parte mică din coaliţia anti-SOPA

şi PIPA.

JACOB: Da, dar stai puţin, că Tumbir, cred, a avut un impact şi mai mare decât a avut Google.

ANDY: Tumbir şi Wikipedia şi mii de acţiuni individuale, acţiuni foarte mici de care poate nu aţi auzit niciodată, au avut un impact. Mii de astfel de acţiuni se aflau în paralel – mergând în aceeaşi direcţie –, iar asta este, din nou, acţiune politică descentralizată. Este o mişcare politică descentralizată la care am fost martori. S-

ar putea ca Google să fi fost doar cel mai mare actor pe care l-ai observat între ceilalţi.

JULIAN: Ei bine, asta a spus Congresul că ar fi observat.

JACOB: Eu am o mică problemă cu ceea ce a spus Jérémie înainte, pentru că, în esenţă, promovezi ideea unei avangarde politice. Nu cred că era intenţia ta să faci lucrul ăsta, dar l-ai făcut şi vreau doar să te opresc în loc, pentru că mişcarea peer-to-peer se împotriveşte în mod explicit unei avangarde politice. Ea reprezintă ideea că suntem cu toţii egali şi că putem distribui între noi; am putea furniza servicii diferite sau am putea furniza funcţionalitate diferită. Ross Anderson mi-a spus odată: „Când m-am alăturat mişcării peer-to-peer, acum cincizeci de ani”, ceea ce mi s-a părut un început fantastic de propoziţie. Mi-a explicat că vrea să se asigure că nu vom dezinventa niciodată presa de tipar. Pentru că pe măsură ce începem să centralizăm serviciile, pe măsură ce începem să centralizăm controlul asupra sistemelor de informaţie, în realitate chiar începem să dezinventăm presa de tipar, în sensul că *Enciclopedia Britannica* nu mai tipăreşte cărţi, ci doar imprimă CD-uri – dacă nu ai un computer cu scop generalist care poate citi acele CD-uri, nu ai acces la acea cunoaştere. Acum, ceea ce se întâmplă în cazul *Enciclopediei Britannica* nu contează, pentru că avem Wikipedia şi avem mult alt material. Dar nu cred că suntem pregătiţi, ca societate.

ANDY: Nu sunt sigur că Wikipedia este atât de bună ca resursă, dacă e să facem o comparaţie. Nu am încredere în nicio pagină de acolo pe care să nu o fi rescris eu.

JACOB: Dar *Enciclopedia Britannica* nu e diferită. Este doar o sursă între multe altele, iar ceea ce contează

este verificarea datelor. Tot ceea ce vreau să spun este că nu ar trebui să promovăm ideea unei avangarde, din cauză că este poate periculoasă.

JULIAN: Stai puţin, de ce? Şi eu sunt un fel de avangardist. Care e problema cu ei?

JÉRÉMIE: Eu nu vorbesc despre avangarde, spun doar că avem instrumente noi la îndemână. Vorbeam despre presa de tipar. Un alt vizionar, un prieten de-al meu, Benjamin Bayart, poate mai puţin cunoscut în afara lumii francofone, a spus: „Presa de tipar a învăţat poporul să citească; internetul a învăţat poporul să scrie”.81 Acesta e un lucru foarte nou, aceasta este o posibilitate nouă, ca toată lumea să poată scrie şi să se poată exprima.

AN DY: Da, dar filtrarea devine şi mai importantă în zilele noastre.

JÉRÉMIE: Sigur, pentru că toată lumea vorbeşte şi multă lume spune tâmpenii. După cum îţi va spune academicianul şi activistul

Larry Lessig şi, cred eu, atâţia alţi profesori, învăţăm oamenii cum să scrie, dar când studenţii îşi predau lucrările, peste nouăzeci şi nouă la sută dintre ele sunt de rahat, dar cu toate acestea îi învăţăm să scrie.82 Aşadar, desigur, oamenii spun tâmpenii pe internet – e evident. Dar faptul de a putea să foloseşti această posibilitate pentru a te exprima în public te face cu timpul din ce în ce mai elocvent în felul tău de a vorbi, din ce în ce mai capabil să participi la discuţii complexe. Şi toate fenomenele pe care le descriem sunt construite pe principiul unei complexităţi pe care trebuie să o divizăm în părţi mici pentru a putea să o înţelegem şi să o dezbatem cu calm. Nu este vorba despre o avangardă politică, este vorba despre a canaliza prin sistemul politic această nouă posibilitate de a ne exprima pe care o avem la îndemână, de a ne împărtăşi

gândurile, de a participa la distribuirea cunoaşterii fără să fim membri ai unui partid politic, ai unei companii media sau ai oricărei alte structuri centralizate de care aveai nevoie în trecut pentru a putea să te exprimi.

Internetul şi economia

9

JULIAN: Aş vrea să mă uit la trei libertăţi fundamentale. Când l-am intervievat pe şeful Hezbollah, Hassan Nasrallah...

JACOB: Acolo unde e blestematul ăla de atac cu drone? Ce se întâmplă acolo?

JULIAN: Păi are şi el un fel de arest la domiciliu, pentru că nu poate să părăsească locul secret în care se află.

JACOB: Nu sunt sigur că aş face comparaţia asta. Te rog, nu face comparaţia asta.

JULIAN: E discutabil dacă Hezbollah are ingredientele unui stat – a devenit oare un stat? Acesta este un lucru menţionat în telegramele ambasadei SUA, şi anume că Hezbollah şi-a construit propria reţea de cabluri de fibră optică în sudul Libanului.83 Deci are cele trei ingrediente principale ale unui stat – are controlul forţei armate într-o anumită regiune, are o infrastructură de comunicaţii pe care o controlează şi are o infrastructură financiară pe care o controlează. Şi ne putem gândi la acestea ca la trei libertăţi fundamentale. Libertatea de mişcare, libertatea fizică de mişcare – posibilitatea de a călători dintr-un loc în altul, fără ca armata să se mobilizeze împotriva ta. Ne putem gândi la libertatea de gândire, şi la libertatea de comunicare, care e inclusă în libertatea de gândire – dacă eşti pus în pericol pentru că vorbeşti în public, singurul mod de a-ţi apăra dreptul de a comunica este să comunici în privat. Şi, în sfârşit,

libertatea interacţiunii economice, care se cuplează, de asemenea, ca libertatea de comunicare, cu confidenţialitatea interacţiunii economice. Aşa că hai să vorbim despre aceste idei, care s-au dezvoltat în mişcarea cypherpunk încă din anii ’90, referitoare la încercarea de a furniza această foarte importantă a treia libertate, care este libertatea interacţiunii economice.

JÉRÉMIE: Dar de ce ai avea nevoie doar de trei libertăţi? în Carta Europeană a Drepturilor Fundamentale sunt mai multe.

JULIAN: Confidenţialitatea devine importantă fie dintr-o perspectivă comunitară, adică ai nevoie de confidenţialitate pentru a comunica liber şi a gândi liber, fie ai nevoie de ea, în vreun fel sau altul, pentru interacţiunile tale economice. Deci cred că există mai multe libertăţi derivate, dar acestea – primele trei pe care le-am numit – sunt libertăţile fundamentale din care derivă toate celelalte libertăţi.

JÉRÉMIE: Păi există o definiţie legală a libertăţii fundamentale.

JULIAN: Dar am citit Carta UE şi pot să-ţi spun că este un dezastru total în ceea ce priveşte consensul.

JÉRÉMIE: Da, OK, şi s-au făcut presiuni şi au reuşit să bage şi proprietatea intelectuală în Carta UE.

JULIAN: Tot felul de chestii pur şi simplu demente.

ANDY: Cred totuşi că există un lucru cu care să fim de acord, şi anume acela că sistemul monetar, infrastructura economică de schimb monetar, este foarte proastă în momentul de faţă.

Şi chiar cineva care are doar un cont de ebay va fi întru totul de acord cu lucrul ăsta, pentru că ceea ce face Paypal, ceea ce fac Visa şi MasterCard, este să pună lumea, *de facto*, într-o situaţie de monopol. Un lucru foarte

interesant, aflat tot din telegramele Wikileaks, este acela că guvernul Rusiei a încercat să negocieze o modalitate prin care plăţile Visa şi MasterCard efectuate de cetăţeni ruşi, pe teritoriul Rusiei, să fie procesate în Rusia, iar Visa şi MasterCard au refuzat.84

JULIAN: Da, puterea combinată a ambasadei Americii şi a Visa a fost suficientă pentru a împiedica până şi Rusia să-şi creeze propriul sistem de plată prin cârd pe teritoriul său.

ANDY: Ceea ce înseamnă că până şi plăţile efectuate de cetăţeni ruşi, la magazine ruseşti, vor fi procesate prin centre de date americane. Deci guvernul SUA va avea controlul jurisdicţional, sau cel puţin informaţii din interior.

JULIAN: Da, deci când Putin iese să-şi ia o Cola, peste treizeci de secunde se ştie la Washington.

ANDY: Iar asta, desigur, este o situaţie foarte nemulţumitoare, indiferent dacă-mi place de SUA sau nu. Este pur şi simplu un lucru foarte periculos să ai o locaţie centrală în care sunt stocate toate plăţile, pentru că facilitează tot felul de întrebuinţări ale acelor date.

JACOB: Unul dintre lucrurile fundamentale de care şi-au dat seama activiştii cypherpunk este că arhitectura defineşte într-adevăr situaţia politică, deci dacă ai o arhitectură centralizată, chiar dacă o controlează cei mai cumsecade oameni din lume, ea va atrage ticăloşi, iar acei ticăloşi vor face lucruri cu puterea lor pe care cei care au proiectat-o nu le-ar face. Şi este important să ne dăm seama că lucrul acesta se aplică şi în cazul banilor.

JULIAN: La fel ca puţurile de ţiţei din Arabia Saudită, blestemul ţiţeiului.

JACOB: Oriunde ne-am uita, mai cu seamă în cazul sistemelor financiare, observăm că, de fapt, chiar dacă

oamenii au cele mai bune intenţii, nu contează. Arhitectura este adevărul. Este adevărul internetului în ceea ce priveşte comunicaţiile. Aşa-numitele sisteme de interceptare legală, ceea ce nu e decât un mod drăguţ de a spune spionarea oamenilor…

JULIAN: Este un eufemism, interceptarea legală.

JACOB: Absolut, la fel ca omorul legal.

ANDY: Sau tortura legală.

JACOB: Aţi auzit despre atacurile legale cu dronă împotriva cetăţenilor americani ale preşedintelui SUA, Obama? Când l-a omorât pe fiul de şaisprezece ani al lui Anwar al-Awlaki în Yemen, a fost omor legal, sau *targeted killing*, cum i-au spus ei [asasinare la comandă].85 Aşa-numita interceptare legală este acelaşi lucru – pui pur şi simplu legal înaintea tuturor cuvintelor şi dintr-odată, din cauză că o face statul, devin legitime. Dar, de fapt, arhitectura statului este cea care le permite să facă lucrul ăsta, arhitectura legilor şi arhitectura tehnologiei, tot aşa cum e şi arhitectură sistemelor financiare.

Ceea ce mişcarea cypherpunk şi-a dorit să facă este să creeze sisteme care să ne permită să ne plătim unul pe altul într-un mod cu adevărat liber, în care să nu fie posibil să se intervină. Cum este moneda chaumiană, care este o monedă electronică proiectată după specificaţiile lui David Chaum, cel care a creat elash (o monedă electronică complet anonimă), deşi ai putea să spui că e mai centralizată decât ar fi necesar. Ideea este să creezi o monedă anonimă, diferită de Visa/MasterCard, care este o monedă ce poate fi urmărită. Deşi e construită în jurul unei autorităţi centrale, moneda chaumiană foloseşte protocoale criptografice inventate de David Chaum, pentru a asigura tranzacţii anonime.86

JULIAN: Deci practic cash electronic fără, să zicem,

numere de serie pe bancnote.

JACOB: Sau numere de serie care-ţi permit să stabileşti că este o monedă valabilă, dar nu-ţi permit să ştii neapărat că Julian i-a făcut o plată lui Andy, sau să ştii care a fost suma.

JÉRÉMIE: Este de fapt recrearea cash-ului în lumea digitală.

JULIAN: Crearea unei monede electronice este un lucru important tocmai din cauză că controlul asupra mijlocului de schimb este unul dintre cele trei ingrediente ale unui stat, după cum spuneam referitor la Hezbollah. Dacă sustragi statului monopolul asupra mijloacelor de interacţiune economică, sustragi unul dintre cele trei ingrediente principale ale statului. În modelul statului ca mafie, unde statul este o organizaţie care asigură protecţia sub ameninţarea pedepsei violente, statul scutură oamenii de bani în toate modurile posibile. Controlarea fluxului de monedă este importantă pentru creşterea venitului de către stat, dar este de asemenea importantă pur şi simplu pentru a controla ceea ce fac oamenii – promovând un lucru, inhibând un altul, interzicând complet o anumită activitate sau o organizaţie, sau interacţiunile dintre organizaţii. Aşadar, de exemplu, în cazul extraordinarei blocade financiare împotriva Wikileaks, nu piaţa liberă e cea care a decis să blocheze Wikileaks, pentru că nu există o piaţă liberă – legislaţia guvernului a numit anumiţi actori financiari regi şi nu permite intrarea pe piaţă a altora. Libertatea economică a fost încălcată de către un grup de elită care poate influenţa atât legislaţia, cât şi principiile după care operează aceste bănci.87

ANDY: Aceasta este marea problemă nerezolvată a lumii electronice în ziua de astăzi, şi mă întristează să o spun. Două companii de credit, ambele cu o infrastructură

de plată electronică cu baza în SUA – ceea ce înseamnă accesul la date în jurisdicţia SUA –, controlează majoritatea plăţilor cu cardul de credit de pe planetă. O companie precum Paypal, care e de asemenea sub jurisdicţie SUA, aplică politici SUA, fie că asta înseamnă blocarea vânzării de trabucuri cubaneze de către magazine germane online sau blocarea plăţilor către Wikileaks în jurisdicţii din afara SUA. Asta înseamnă că guvernul SUA are accesul la date şi opţiunea de a impune controale asupra plăţilor din întreaga lume. Deşi cetăţenii americani ar putea susţine că aceasta este cea mai bună democraţie posibilă, pentru cetăţenii europeni lucrul acesta e ridicol.

JULIAN: În lumea tradiţională am avut o anumită libertate de mişcare, nu prea mare în unele cazuri.

JACOB: Eşti sigur, Julian? Am sentimentul că libertatea ta de mişcare este un exemplu elocvent despre cât de liberi suntem cu adevărat.

JULIAN: Păi nu, Regatul Unit a anunţat că va pune 100.000 de oameni pe an în situaţia mea.88 Deci cred că e colateral într-o anumită măsură.

JACOB: Ăsta e motivul pentru care fondatorii ţării mele au împuşcat oameni din Marea Britanie. Avem un motiv bine întemeiat pentru care i-am împuşcat pe britanici. Iar el încă există şi astăzi. Tirania există.

JÉRÉMIE: Hai să nu facem remarci personale.

ANDY: Ceea ce SUA, ţara ta, fac în momentul de faţă, este să privatizeze închisorile administrate anterior de guvern şi să negocieze cu companiile private care administrează aceste închisori contracte ce garantează o rată de ocupare de nouăzeci la sută.89 Păi ce-i asta? Ăsta e capitalismul împins la absurd.

JULIAN: Există mai mulţi oameni în închisorile SUA decât erau în Uniunea Sovietică.

JACOB: Aceasta e eroarea de judecată în care, din cauză că eu protestez împotriva unui lucru greşit, tu poţi sugera că aş face parte dintr-un lucru la fel de greşit. Nu vreau să sugerez că Statele

Unite ar fi perfecte. Cred că Statele Unite sunt destul de faine în multe privinţe, dar mai cu seamă în ceea ce priveşte retorica

Părinţilor Fondatori.

JULIAN: Retorica Părinţilor Fondatori s-a aflat într-o clară disoluţie în ultimii zece ani.

JACOB: Trebuie să nu pierdem din vedere faptul că o mare parte din percepţia despre retorica Părinţilor Fondatori este mitologie şi că ar trebui să fim atenţi să nu-i idolatrizăm. Deci da, desigur. Tot ceea ce am vrut să spun, prin comentariul meu despre tirania britanică şi despre situaţia în care se află Julian, este că acest lucru este în realitate o chestie culturală. Aici intră în scenă societatea şi y aici societatea este foarte importantă, şi este foarte dificil ca tehnologia să înlocuiască acest lucru. Iar chestiunile financiare sunt lucrul cel mai periculos de care să te ocupi. Există un motiv bine întemeiat pentru care cel care a creat o altă monedă electronică, Bitcoin, a făcut-o anonim. Nu vrei să fii cel care inventează prima monedă electronică de succes.90

JULIAN: Băieţii care au inventat e-gold au sfârşit prin a fi urmăriţi penal în SUA.91

JACOB: Este foarte frustram.

JULIAN: Aş vrea să mă întorc la aceste trei libertăţi fundamentale: libertatea de a comunica, libertatea de mişcare şi libertatea interacţiunii economice. Dacă ar fi să ne uităm la trecerea la internet a societăţii noastre globale, când am făcut acea trecere, libertatea de mişcare

personală a rămas neschimbată, practic. Libertatea de a comunica a sporit într-o manieră uluitoare în anumite privinţe, în sensul că acum putem comunica cu mult mai mulţi oameni; pe de altă parte, s-a şi degradat într-o manieră uluitoare, pentru că nu mai există confidenţialitate, iar astfel comunicarea noastră poate fi spionată, şi chiar este spionată şi stocată şi, în consecinţă, poate fi folosită împotriva noastră. Şi astfel, acea interacţiune elementară pe care o avem în mod fizic cu oamenii este degradată şi ea.

ANDY: Confidenţialitatea este posibilă, dar are un cost.

JULIAN: Interacţiunile noastre economice au avut de suferit aceleaşi consecinţe. Căci în cazul unei interacţiuni economice tradiţionale, cine ştie de ea? Cei care te-au văzut că ai mers la piaţă. Dar acum, cine ştie despre interacţiunea ta economică? Dacă cumperi ceva de la vecinul tău cu cardul Visa, lucru pe care, într-o societate tradiţională de piaţă, ai fi putut să-l faci aproape complet în privat, cine ştie acum despre asta?

JACOB: Toată lumea.

JULIAN: Toată lumea ştie. Distribuţia de date se face între toate marile puteri occidentale, toate ştiu despre asta şi stochează datele pentru totdeauna.

ANDY: Julian, ceea ce spui tu nu este fals, dar nu sunt sigur că putem face cu adevărat distincţie între libertatea de a comunica şi libertatea interacţiunii economice, din cauză că internetul, aşa cum îl avem astăzi, este infrastructura pentru interacţiunile noastre sociale, economice, culturale, politice, pentru toate interacţiunile noastre.

JACOB: În mod cert libertatea de mişcare.

ANDY: Oricare ar fi arhitectura comunicaţiilor, banii

sunt doar biţi. Este doar folosire a internetului. Deci dacă sistemul economic este bazat pe infrastructura electronică, atunci arhitectura infrastructurii electronice spune ceva despre cum are loc fluxul monetar, despre cum este el controlat, cum este centralizat şi aşa mai departe. Poate că internetul nici nu a fost gândit, în primele zile ale existenţei sale, ca o infrastructură pentru orice, dar logica economică spune: „Păi, este mai ieftin să facem cutare lucru cu internetul”. Băncile şi companiile de carduri de credit aveau bancomate dinainte, cu interfeţe X.25, ceea ce constituia o reţea separată acum zece sau douăzeci de ani, iar acum totul este TCP/ IP pentru că e mai ieftin.92 Deci arhitectura tehnologiei devine o chestiune-cheie din cauză că afectează toate celelalte arii, iar de asta avem nevoie pentru a regândi cu adevărat lucrurile, în sensul că dacă vrem o modalitate economică descentralizată de a ne administra plăţile, trebuie să preluăm infrastructura.

JACOB: Bitcoin este în esenţă o monedă electronică.

ANDY: Fără inflaţie.

JACOB: Tinde să o facă într-o manieră descentralizată, deci în loc să ai Sistemul Federal de Rezervă Monetară, ai o mână de oameni în toată lumea care hotărăsc de comun acord care e realitatea şi care e moneda lor curentă.

J U LI AN: Şi există şi programe de calculator care facilitează lucrul acesta.

JACOB: Vreau să explic asta într-o manieră care nu este tehnică. Este o monedă electronică care este mai degrabă o marfă decât o monedă, în sensul că oamenii stabilesc câţi euro are un Bitcoin* Deci este un pic ca aurul în acest sens şi mai există şi costul aşa-numitei extracţii a Bitcoin-ului, unde operezi o căutare pe un computer pentru a găsi un Bitcoin, şi ideea este că există o complexitate a

calculelor şi că ea este legată de valoarea lucrului. Deci în termeni non-tehnici este o modalitate ca eu să-i trimit bani lui Julian fără ca Andy să fie în stare să intervină sau să oprească tranzacţia. Există şi unele probleme, însă – nu este în realitate o monedă anonimă, iar acesta este un lucru nesatisfăcător, în opinia mea.

JULIAN: Bitcoin este un hibrid foarte interesant, pentru că deţinătorii de conturi sunt în întregime anonimi şi pentru că poţi să-ţi faci un cont oricând doreşti, dar tranzacţiile întregii economii Bitcoin sunt complet publice. Şi aşa funcţionează ea; trebuie să fie aşa, pentru ca toată lumea să poată verifica dacă o tranziţie s-a produs, dacă contul expeditor are acum mai puţini bani, iar cel destinatar are mai mulţi. Aceasta este una dintre puţinele modalităţi în care poţi permite funcţionarea unui sistem monetar Online care nu necesită un server central, fiindcă acesta ar putea fi o ţintă atrăgătoare pentru controlul coercitiv. Dar distribuţia este cea care este cu adevărat inovatoare în cazul Bitcoin, şi algoritmii care permit distribuţia, în sensul că nu te încrezi anume în vreuna dintre părţile reţelei bancare Bitcoin, ca să-i spunem aşa. Ci încrederea este distribuită. Iar funcţionarea regulamentară a sistemului nu se face prin legi sau reguli sau controale, se face prin dificultatea calculului criptografic prin care trebuie să treacă fiecare parte a reţelei pentru a dovedi că face ceea ce susţine că face. Deci funcţionarea regulamentară a unui „sistem bancar” onest bazat pe Bitcoin este integrată în arhitectura sistemului. Calculul se traduce în costuri de electricitate pentru fiecare ramură a băncii Bitcoin, deci fraudarea poate să aibă un cost, în termenii preţului la electricitate. Lucrurile sunt stabilite în aşa fel încât munca necesară comiterii unei fraude să presupună costuri de electricitate

mai mari decât beneficiul economic care rezultă din ea. Este foarte inovativ, nu pentru că aceste idei nu ar fi fost explorate înainte (ele au existat timp de douăzeci de ani, pe hârtie), ci pentru că Bitcoin a găsit echilibrul perfect şi a adăugat o idee foarte inovativă despre cum să atingi un adevărat consens global cu privire la tranzacţiile economiei Bitcoin, chiar pornind de la prezumţia că multe bănci sunt frauduloase şi că oricine ar putea fonda una.

Desigur, la fel ca oricare altă monedă, trebuie să cumperi această monedă cu altceva, cu muncă, sau Bitcoin-ul poate fi schimbat cu o altă monedă – există grupări de schimb valutar care fac asta. Mai sunt şi alte limitări. Are o perioadă de achitare a plăţii de circa zece minute – e nevoie de aproximativ zece minute de activitate de calcul între transferul de monedă şi asigurarea de către a doua parte că există un consens global asupra efectuării tranzacţiei. Este exact ca o monedă fizică, aşa că are toate problemele legate de furt pe care le are moneda fizică. Are de asemenea şi toate avantajele: odată ce ai primit banii, poţi fi sigur că ai fost plătit, cecul nu poate fi anulat, banca nu-l poate retrage. Relaţiile de forţă coercitivă le taie legăturile. Pe de altă parte, trebuie să păzeşti bine moneda. Aceasta este, cred eu, cea mai mare problemă a sa. Dar este destul de uşor să adaugi mai multe straturi deasupra, să construieşti servicii de împuternicire legală prin care să-ţi stochezi banii într-un server care este conceput anume pentru a-i păstra în siguranţă şi pentru a-i asigura împotriva furtului.

JACOB: Ce este interesant e că dacă cei care au creat Bitcoin ar fi stabilit ca Tor să fie folosit în mod obligatoriu de toată lumea, astfel încât să nu-ţi creezi un cont, ci să creezi nişte identificatoare criptografice, ar fi fost posibil, dacă totul ar fi trecut prin Tor ca structură internă a

întregului sistem, să ai confidenţialitate a locaţiei, chiar dacă ai fi avut totuşi identificatori folosiţi pe termen lung care te identificau ca să-ţi poţi lega tranzacţiile unele de altele.

JÉRÉMIE: Fără să intrăm în chestiuni de ordin tehnic, am putea cădea cu toţii de acord că Bitcoin are la bază concepte excelente, dar şi unele neajunsuri. Are o natură deflaţionistă, pentru că banii tind să dispară de pe Bitcoin. Deci nu poate funcţiona pe termen lung, dar introduce concepte care pot fi îmbunătăţite. E probabil versiunea O.7 sau O.8 acum.

JACOB: Este ca şi cum ai reinventa David Chaum.93

ANDY: Bitcoin reprezintă încercarea de a introduce o monedă digitală care a înregistrat cel mai mare succes din ultimii zece ani, aş spune eu.

JULIAN: Aproape că au descoperit echilibrul perfect. Eu cred că Bitcoin va continua. Este o monedă eficientă; poţi să-ţi deschizi un cont în zece secunde, iar pentru a transfera bani de acolo nu suporţi alte cheltuieli decât costul unei conexiuni la internet şi a câtorva minute de electricitate. Este foarte competitiv în comparaţie cu oricare altă modalitate de transfer monetar. Cred că va prospera. Uitaţi-vă doar la ce s-a întâmplat în urma unor furturi de Bitcoin şi a unor recenzii negative în presă, în vara lui 2011, care au coborât rata de schimb la trei dolari SUA.94 Bitcoin s-a ridicat treptat înapoi la doisprezece dolari. Nu a crescut brusc, nu şi-a revenit dintr-un singur salt, ci s-a ridicat într-un mod gradual care pare să indice o cerere crescândă pentru această monedă. Suspectez că o mare parte din această cerere se datorează micului trafic de droguri, comenzilor de marijuana prin poştă şi aşa mai departe.95 Dar Bitcoin are cheltuieli mici ca monedă. Mai multe ISP-uri încep să o folosească, mai cu seamă în ţări în

care nu ai acces uşor la servicii de card de credit, cum ar fi fosta Uniune Sovietică.

Vor exista măsuri împotriva ei dacă va continua să crească. Nu vor putea să elimine moneda Bitcoin, din cauză că procedeele criptografice împiedică reuşita oricărui atac coercitiv, dar genul de servicii de schimb valutar care schimbă în şi din Bitcoin vor putea H împiedicate mult mai uşor să funcţioneze. Pe de altă parte, aceste schimburi valutare pot funcţiona oriunde în lume, deci sunt destule jurisdicţii prin care trebuie să treci ca să nu mai existe servicii de schimb valutar şi, de asemenea, piaţa neagră are propria sa logică în materie de schimb valutar. Eu cred că modul în care trebuie abordată moneda Bitcoin este să se încerce ca ea să fie adoptată de ISP-uri şi de industria serviciilor de internet pentru genul de jocuri mici, pe care le cumperi pe Facebook şi aşa mai departe, din cauză că este atât de eficientă, şi, odată ce a fost adoptată de mai multe industrii, ele vor forma un lobby pentru a împiedica interzicerea ei. Este, într-un fel, modul în care a fost adoptată criptografia. La început a fost inclusă în aceeaşi categorie cu comerţul de arme, iar unii dintre noi au fost numiţi comercianţi de arme, dar odată ce a fost în browsere şi a fost folosită pentru servicii bancare, s-a creat un lobby destul de puternic pentru a-i împiedica interzicerea – deşi mă văd nevoit să recunosc că sunt din nou în pregătire mişcări în acest sens.

JACOB: Problema este că îngrijorările legate de confidenţialitate sunt false. Hai să fim cinstiţi. Este fals să sugerezi că aspectele economice ale situaţiei de faţă sunt altfel cu internet decât fără internet. Când am ajuns aici şi am cumpărat lire sterline a trebuit să predau CNP-ul, care este identificatorul meu unic în Statele Unite, a trebuit să-mi predau numele, a trebuit să conectez numele şi contul

bancar, a trebuit să le dau banii. Au înregistrat toate numerele de serie şi apoi au luat toate acele informaţii şi le-au transmis guvernului federal. Deci aceasta e analogia. De fapt, este mai greu să cumperi valută străină în SUA, din cauză că suntem atât de îndepărtaţi de toate celelalte ţări. Dar există o tendinţă istorică în ceea ce priveşte controlul monedei şi nu vedem acest control doar în legătură cu internetul. Mai mult decât atât, am înţeles că există bancomate în unele bănci care înregistrează numerele de serie ale bancnotelor, iar apoi le urmăresc, pentru a face analize de flux al bancnotelor, pentru a vedea unde au fost cheltuite şi cine ce a făcut cu ele.

Dacă ne uităm la aceste sisteme, iar apoi ne întoarcem privirea la internet, nu au îmbunătăţit confidenţialitatea, pe măsură ce am migrat către internet – de fapt, au păstrat-o la fel de proastă cum era înainte. În acest sens, cred că este foarte important să ne uităm la tendinţele din lumea de dinaintea internetului pentru a vedea încotro ne îndreptăm. Ceea ce observăm este că dacă ai mulţi bani poţi plăti o taxă pentru a-ţi păstra confidenţialitatea, iar dacă nu ai mulţi bani, e aproape garantat că nu ai confidenţialitate. Şi este şi mai rău în cazul internetului. Lucrurile ca Bitcoin sunt un pas în direcţia corectă, fiindcă atunci când este combinat cu un canal anonim de comunicaţii, cum ar fi Tor, de pildă, îţi permite să trimiţi un Bitcoin către Wikileaks prin intermediul sistemului Tor, şi oricine ar privi această tranzacţie ar vedea un utilizator Tor trimiţând un Bitcoin, iar pe tine primindu-l. Este posibil lucrul acesta – în unele privinţe este mult mai bun decât moneda clasică.

JULIAN: Cu toţii vorbim despre confidenţialitatea comunicaţiilor şi dreptul de a publica. Acestea sunt lucruri destul de lesne de înţeles – au o istorie lungă în spatele lor

– şi, în realitate, jurnaliştii adoră să vorbească despre ele pentru că-şi protejează propriile interese. Dar dacă am compara valoarea lor cu valoarea confidenţialităţii şi libertăţii interacţiunilor economice, de fapt, de fiecare dată când CIA urmăreşte o interacţiune economică, ei pot vedea că este din partea cutarei persoane, din cutare loc, către cutare persoană în cutare loc şi pot să estimeze astfel valoarea şi importanţa interacţiunii. Deci nu este cumva libertatea sau confidenţialitatea interacţiunilor economice mai importantă decât libertatea de exprimare, din cauză că interacţiunile economice se află la baza întregii structuri a societăţii?

JACOB: Ele sunt legate intrinsec. Cred că aici se poate observa diferenţa dintre activiştii cypherpunk americani şi cei europeni, din cauză că majoritatea activiştilor americani ar spune că ele sunt acelaşi lucru. Fiindcă într-o societate cu o economie de piaţă liberă, ai putea spune că-ţi demonstrezi vorbele prin fapte.

JULIAN: Dar o faci urmărind în acelaşi timp să-ţi consolidezi puterea.

JACOB: Exact. Nu vreau să spun că e corect aşa, e aproape o atitudine de dreapta faţă de chestiunea asta, care poate nu este ceea ce vrem noi. Poate vrem un capitalism social, de exemplu.

JULIAN: Dacă ar fi să ne uităm doar dintr-o perspectivă de spionaj: ai un buget de 10 milioane de dolari. Poţi spiona interacţiunile pe e-mail ale oamenilor sau le poţi supraveghea toate interacţiunile economice. Ce preferi?

ANDY: Păi, în zilele noastre ar spune: „Bine, vom obliga companiile de plăţi şi băncile să folosească internetul, şi astfel împuşcăm amândoi iepurii”. Şi asta este chiar ceea ce au făcut. Deci concluzia este că nu mai

există o scăpare directă. Poţi să foloseşti Tor, de exemplu, pentru a-ţi proteja comunicaţiile, poţi să-ţi criptezi convorbirile telefonice, poţi să-ţi securizezi mesageria. În privinţa banilor, lucrurile sunt mult mai complicate şi există de pildă legi împotriva spălării de bani şi aşa mai departe, şi ni se spune că organizaţiile teroriste şi de trafic de droguri abuzează de infrastructură pentru a face rău.

JACOB: Sunt Călăreţii Apocalipsei Informatice.

ANDY: De fapt, aş fi foarte interesat să avem mai multă transparenţă în privinţa cheltuielilor efectuate de companiile de supraveghere şi de guverne pentru aceste chestiuni. Întrebarea este ce avem de câştigat dacă acordăm anonimitate totală doar sistemului monetar? Ce s-ar întâmpla în realitate? Eu cred că lucrul acesta ar putea conduce ici şi colo la fenomene interesante în care oamenii ar putea să-şi uşureze puţin situaţia şi să spună: „Păi, ştii, aş putea să-mi ridic vocea, aş putea să merg în Parlament, dar aş putea la fel de bine să mituiesc nişte politicieni”.

JÉRÉMIE: Descrii situaţia din SUA, nu-i aşa?

JACOB: Nu e anonim.

AN DY: Nu sunt atât de sigur că situaţia e doar a SUA. în Germania nu-i spunem corupţie, spunem că sunt fundaţii care cumpără tablouri ale soţiilor politicienilor, aşa că vorbim de comerţul de artă şi de diverse alte domenii. Deci avem denumiri mai bune. S-ar putea ca în Franţa să i se spună petreceri ale prieteniei, iar alţii să-i spună angajare de prostituate.

JÉRÉMIE: În SUA este un caz special, din cauză că legătura dintre sistemul politic şi bani e foarte strânsă. După ce a lucrat zece ani în domeniul drepturilor de autor, Larry Lessig a spus că a renunţat să mai încerce să remedieze problema drepturilor de autor (de fapt, nu a renunţat), din cauză că şi-a dat seama că problema n-o

reprezenta opinia politicienilor despre ce înseamnă o politică bună de copyright, problema era că există pur şi simplu prea multe legături cu actorii industriali care încearcă să instaureze un regim prost ai drepturilor de autor.96 Deci avem aici o problemă cât se poate de reală.

JULIAN: Eşti sigur că este o problemă, Jérémie? Poate că de fapt este o însuşire bună aceea că industriile care sunt productive…

ANDY: Cred că avocatul diavolului îmi bea din whisky.

JACOB: Hai să vedem dacă poate termina propoziţia asta fără să izbucnească în râs. Provoacă-ne, Maestre Provocator.

JULIAN: Acele industrii care sunt productive, care produc bogăţie pentru întreaga societate folosesc o parte din banii lor pentru a se asigura că rămân productive, înlăturând legislaţiile aiurea care se nasc dintr-o mitologizare politică, rezultat al exagerărilor. Iar cea mai bună modalitate de a face asta chiar este să mituieşti membri ai Congresului, să foloseşti activitatea industriei productive pentru a modifica legea – astfel încât să menţii productivitatea industriei.

JACOB: Staţi – am să răspund eu la asta. Sunteţi gata? Sunteţi gata? Acum, sunteţi gata? Nu.

JULIAN: De ce?

JACOB: Sunt mai multe motive, dar, în primul rând, există o buclă de reacţie extrem de negativă. De exemplu, cred că unul dintre cei mai mari sponsori de campanie din statul California este sindicatul paznicilor de închisoare, şi asta pentru că vor să facă lobby pentru legi mai dure – nu fiindcă ar fi interesaţi de domnia legii, ci fiindcă aşa ceva ar fi în avantajul meseriei lor.97 Deci dacă vezi că oamenii aceştia fac lobby pentru construirea mai multor închisori, pentru închiderea mai multor oameni, pentru prelungirea

duratei sentinţelor, ce fac ei în realitate? Ceea ce fac ei este să se folosească de câştigurile pe care le au de pe urma activităţii lor benefice – indiscutabil – pentru a extinde monopolul pe care li-l acordă statul.

JULIAN: Deci se folosesc de asta pentru a transfera banii de la industiile productive la cele care nu produc nimic?

JACOB: Ai putea să spui şi aşa.

JULIAN: Dar poate că asta este doar o componentă minoră. De orice sistem se abuzează, poate că aceşti profitori care se ocupă doar cu transferurile de bani reprezintă un element minor şi, de fapt, cea mai mare parte a lobby-ului, cea mai mare influenţă asupra Congresului vine din partea industriilor productive, care se asigură că legile vor continua să permită acestor industrii să fie productive.

JACOB: Dar poţi măsura lucrul ăsta foarte uşor, fiindcă poţi căuta care sunt oamenii care doresc să promoveze activităţi de tipul *rent-seeking* şi care vor să restricţioneze libertatea altor oameni pentru a crea o situaţie în care ei înşişi nu ar fi putut să se ridice la nivelul la care sunt astăzi. Când fac lucruri de genul acesta ştii că ceva nu este în regulă şi că pur şi simplu încearcă să apere lucrurile pe care le au, lucruri pe care le-au agonisit, în principal, printr-o exploatare – de regulă, printr-un apel la emoţii prin care spun: „Vai, opriţi teroristul, opriţi pornografia infantilă, opriţi spălarea de bani, declaraţi război drogurilor”. Se poate ca aceste lucruri să fie cât se poate de rezonabile în contextul în care au fost prezentate iniţial, şi de regulă chiar sunt, fiindcă, în general vorbind, credem că aceste lucruri sunt rele pentru că există un element grav în fiecare dintre ele.

ANDY: Aş vrea să mă întorc la chestiunea drepturilor

de autor şi să vă mai dau un exemplu – au existat probleme serioase când au apărut automobilele. Cei care conduceau companii de transport al pasagerilor cu ajutorul cailor se temeau că asta avea să le ucidă afacerea, lucru care s-a întâmplat, dar poate că avea şi o logică. Am fost invitat să vorbesc la asociaţia companiilor de film din Germania, iar înaintea discursului meu a fost un profesor al unei universităţi din Berlin care a vorbit foarte politicos despre evoluţia rasei umane şi dezvoltarea culturii, spunând că copierea gândurilor şi procesarea lor ulterioară sunt elementul-cheie, tot aşa cum regia de film ţine de preluarea unor teme şi exprimarea lor într-o manieră dramaturgică. După cele patruzeci de minute pe care le avea la dispoziţie, moderatorul l-a întrerupt cu neobrăzare şi a spus: „Ok, după ce tocmai aţi spus că trebuie să legalizăm furtul, haideţi să vedem ce are să ne spună tipul de la Chaos Computer Club”. Şi m-am gândit: „Wow, ce căcat? Dacă e să-mi spun răspicat părerea, o să mai ies întreg de aici?” Deci unele industrii au pur şi simplu pledoarii care nu slujesc evoluţiei. E un mod egoist de a proceda, faptul că se blochează în abordarea lor antievoluţionistă care face ca totul să fie şi mai monopolizat. Şi când au apărut casetele au crezut că industria muzicală va dispărea. S-a întâmplat opusul, industria a explodat. Întrebarea e care e politica aici? Care este modalitatea pozitivă în care ai putea formula aceste lucruri?

JULIAN: Mă întreb dacă nu am putea, de fapt, să standardizăm practica actuală din Statele Unite şi să o legiferăm astfel încât pur şi simplu să mituieşti senatori şi să cumperi voturi în Senat.

JÉRÉMIE: Nu, nu, nu, nu.

AN DY: Hai să presupunem că avem banii necesari.

JULIAN: Da, şi că totul este pe faţă şi că există cumpărători şi că fiecare merge la o licitaţie.

AN DY: Dar industria de armament ar avea oricum mai mulţi bani.

JULIAN: Nu, cred că nu ar avea. Cred, de fapt, că complexul militaro-industrial ar fi relativ marginalizat, deoarece capacitatea lor de a funcţiona în spatele uşilor închise, într-un sistem care nu este deschis procesului de licitaţii de piaţă, este mai mare decât a altor industrii.

JACOB: Există o inegalitate fundamentală în sistem.

JÉRÉMIE: Dintr-o perspectivă economică liberală, antimonopol, când spui hai să lăsăm actorii dominanţi să decidă care va fi politica, îţi pot răspunde pe baza experienţei internetului ultimilor cincisprezece ani, unde inovaţia se producea prin aşa-numitul sistem de jos în sus, unde practici noi apăreau de nicăieri, unde doi tipiinventau o tehnologie de succes într-un garaj.

JULIAN: Aproape totul, Apple, Google, YouTube, totul.

JÉRÉMIE: Totul. Tot ceea ce a apărut pe internet a explodat pur şi simplu după ce cu câteva luni sau câţiva ani înainte fusese necunoscut, deci nu poţi să prezici care ar putea fi următoarea inovaţie, iar ritmul inovaţiilor este atât de rapid, încât este mult mai rapid decât procesul de elaborare de politici. Deci când elaborezi o lege care să aibă un impact asupra pieţei aşa cum e ea astăzi, asupra relaţiilor de putere dintre diferitele companii şi actori economici aşa cum se prezintă ei astăzi, dacă acorzi mai multă putere cuiva care este deja puternic, poţi bloca apariţia unui nou actor care ar fi fost mai eficient.

JULIAN: Piaţa trebuie să fie reglementată pentru a fi liberă.

JÉRÉMIE: Fireşte că trebuie să lupţi împotriva

monopolurilor şi că ai nevoie de o putere care să fie superioară puterii companiilor în cauză pentru a putea pedepsi comportamentele neregulamentare – dar ceea ce vreau să spun aici este că politicile trebuie să se adapteze la societate, nu invers. În cazul războaielor Copyright avem impresia că legislatorul încearcă să schimbe întreaga societate pentru a se adapta la un şablon definit de Hollywood, de exemplu. „Uitaţi care e treaba, ceea ce faceţi acum, cu noile practici culturale, este pur şi simplu greşit din punct de vedere moral, iar dacă nu vreţi să încetaţi, vom elabora instrumente legale care să vă facă să încetaţi a mai face ceea ce credeţi voi că e bine”. Nu aşa se elaborează o politică bună. O politică bună priveşte lumea şi încearcă să se adapteze, astfel încât să corecteze ceea ce este greşit şi să permită în continuare ceea ce este bine. Sunt convins că atunci când le permiţi celor mai puternici actori economici să decidă în privinţa politicilor, nu urmezi calea asta.

AN DY: Eu încerc pur şi simplu să vă stimulez să vă gândiţi – şi eu împreună cu voi – care ar fi o politică bună. Ceea ce ai formulat tu mi se pare, în momentul de faţă, puţin prea complicat. Încerc să simplific puţin lucrurile. Există un tip pe care-l cheamă Heinz von Foerster – naşul ciberneticii – care a elaborat la un moment dat un set de reguli, iar una dintre aceste reguli era „Acţionează tot timpul în aşa fel încât să sporeşti opţiunile”.98 Aşadar, în cazul politicilor, al tehnologiei, a orice, fa tot timpul ceea ce-ţi aduce mai multe, nu mai puţine opţiuni.

JULIAN: Şi în cazul strategiei de şah e la fel.

ANDY: S-a spus că amplificarea confidenţialităţii tranzacţiilor monetare ar putea avea un efect negativ, aşa că trebuie să ne gândim: „În momentul de faţă, sistemul monetar are o logică specifică şi chestiunea importantă

este cum împiedicăm sistemul monetar să invadeze alte arii de activitate”. Fiindcă sistemul monetar are posibilitatea – spre deosebire de sectorul de comunicaţii – să afecteze şi să limiteze opţiunile pe care le au oamenii în alte arii de activitate. Dacă poţi plăti asasini pentru a face anumite lucruri, sau dacă îţi poţi cumpăra arme şi merge la război împotriva altor ţări, atunci limitezi opţiunile altor oameni de a trăi, de a acţiona. Dacă investesc mai mulţi bani în comunicaţii, atunci mai mulţi oameni ar avea mai multe opţiuni. Dacă aduc pe piaţă mai multe arme…

JACOB: Nu – cu cât ai o mai mare posibilitate de a supraveghea, cu atât ai mai mult control.

ANDY: Ceea ce reprezintă încă un argument bun pentru a restricţiona piaţa de armament, inclusiv tehnologia de supraveghere a telecomunicaţiilor.

JACOB: Da, sigur, vrei să-mi restricţionezi capacitatea de a vinde lucrurile acestea, dar cum o vei face? Cum îmi poţi restricţiona capacitatea de a transfera bogăţii? – tot prin reţelele de comunicaţii. În Statele Unite, unul dintre cele mai ofensatoare aspecte legate de sprijinele financiare[5] acordate – ofensatoare pentru mulţi oameni, dintr-o mulţime de motive – a fost faptul că au arătat că banii nu sunt nimic mai mult decât o serie de biţi într-un sistem informatic. Unii oameni, cerşind într-un mod foarte eficient, au reuşit să determine creşterea valorii multora dintre aceşti biţi, şi atunci care e întrebarea? Are vreo valoare sistemul dacă poţi trişa pur şi simplu şi creşte valoarea biţilor tăi? Iar tuturor celorlalţi care să străduiesc să se descurce nu le este recunoscut faptul că au şi ei biţi care merită să fie măcar luaţi în considerare”.

---

5 Este vorba despre aşa-numitele „bailouts“, sprijine financiare acordate de guvernul SUA unor companii sau ţări aflate în dificultate financiară sau în faliment. (n.tr.)

ANDY: Deci ceea ce vrei tu să spui este că avem nevoie de un sistem economic complet diferit? Pentru că în ziua de astăzi valoarea nu este legată de valoarea economică.

JACOB: Nu, spun că există o valoare economică.

ANDY: Poţi face bani din ticăloşii, şi poţi produce lucruri bune fără să iei un sfanţ pe ele.

J ACOB: Păi nu, ceea ce vreau să spun este că nu poţi să decuplezi economia de comunicaţii. Nu spun că avem sau nu nevoie de un alt sistem economic. Nu sunt economist. Voi spune doar că sistemele de comunicaţii şi libertatea acelor comunicaţii au o oarecare valoare, la fel cum libertatea schimbului în natură are o valoare – am dreptul să-ţi dau ceva în schimbul muncii tale, la fel cum am dreptul să-ţi explic o idee, iar tu ai dreptul să-mi spui ce crezi despre ideea mea. Nu putem spune că sistemul economic se află într-un soi de vid. Sistemul de comunicaţii este legat de el în mod direct, iar lucrul ăsta face parte din societate.

Dacă e să avem această noţiune reducţionistă despre libertate, despre cele trei libertăţi pe care le-a menţionat Julian, aceasta este legată în mod evident de libertatea de mişcare – astăzi nu poţi nici măcar să-ţi cumperi un bilet de avion fără să foloseşti o monedă care poate fi urmărită, fiindcă în caz contrar vei fi însemnat cu un steguleţ. Dacă intri într-un aeroport şi încerci să-ţi cumperi un bilet în aceeaşi zi cu bani în numerar, vei fi însemnat. Vei fi supus unor proceduri de verificare suplimentare, nu vei putea zbura fără a te fi legitimat, iar dacă ai avut ghinionul să-ţi cumperi biletul de avion cu cardul de credit, vor înregistra totul despre tine – de la adresa ta de IP până la browserul folosit. Eu chiar am datele mele, obţinute conform Legii libertăţii informaţiei, din arhiva Serviciului pentru

Controlul Imigraţiei şi Normelor Vamale de acum câţiva ani, pentru că m-am gândit că va fi interesant să mă uit la diferenţe într-o bună zi. Şi, ca să vezi, e inclus acolo şi Roger Dingledine, care mi-a cumpărat un bilet de avion pentru o chestie legată de muncă, e inclus cârdul său de credit, adresa locului în care se afla când l-a cumpărat, browserul pe care l-a folosit şi toate informaţiile despre biletul de avion, toate înregistrate împreună.

JULIAN: Şi toate acestea au mers către guvernul SUA, nu au fost doar stocate în procesorul comercial?

JACOB: Exact. Datele comerciale au fost colectate, trimise către guvern şi au fost stocate împreună. Iar lucrul care mi s-a părut complet nebunesc este că, în esenţă, este vorba despre fuzionarea acestor trei lucruri de care vorbeşti tu. Era dreptul meu să călătoresc liber, era capacitatea mea să cumpăr acel bilet de avion sau ca altcineva să-l cumpere, şi era vorba, efectiv, de capacitatea mea de a mă exprima – călătoream pentru a ţine un discurs undeva, iar pentru a face acel lucru a trebuit să fac compromisuri în celelalte două sfere. Şi de fapt îmi lezează capacitatea de a mă exprima, mai cu seamă când aflu mai târziu ce au colectat şi faptul că au stocat totul la un loc.

Cenzura

J U LI AN: Jake, poţi să spui câte ceva despre faptul că ai fost reţinut în aeroporturile SUA şi despre motivul pentru care s-a întâmplat?

JACOB: Mi-au spus că se întâmplă din cauză că „ştiu eu de cca.

JULIAN: Dar n-au spus de ce?

ANDY: Pot să încerc eu să rezum chestiunea, fiindcă securitatea tehnică şi securitatea afacerilor guvernamentale sunt două lucruri complet distincte. Poţi avea un sistem tehnic cât se poate de securizat şi guvernul

va crede că nu este bun de nimic, pentru că ei cred că securitatea este atunci când pot observa ce se întâmplă în interiorul său, când îl pot controla, când pot sparge securitatea tehnică. Ceea ce s-a întâmplat nu s-a întâmplat din cauză că Jake ar fi încercat să se apropie de vreun avion, să omoare pe cineva, să deturneze un avion sau mai ştiu eu ce. A fost vorba despre capacitatea sa de a afecta afacerile guvernamentale călătorind în alte ţări, comunicând cu oamenii, răspândind idei. Acesta este cel mai periculos lucru care se poate întâmpla unui guvern în ziua de astăzi – când ideile oamenilor sunt mai bune decât politica lor.

JACOB: Apreciez foarte mult complimentul pe care mi l-ai făcut prin afirmaţia asta, dar aş vrea să subliniez că ceea ce s-a întâmplat este mult mai rău decât atât, pentru că de la toată lumea se colectează genul acesta de date. Aceasta s-a întâmplat înainte să fi făcut eu ceva interesant; era vorba despre simplul fapt că plecam într-o călătorie, iar sistemele însele, arhitectura, promovau colectarea aceasta de informaţii. Aceasta s-a întâmplat înainte să fi fost oprit pentru ceva, înainte să fi fost deportat din Liban, înainte ca guvernul SUA să fi avut vreun interes special faţă de mine.

ANDY: Poate au prevăzut ceva, poate au observat ceva înainte să o fi făcut tu.

JACOB: Bineînţeles, în parte din cauza colectării acestor date. Dar de fiecare dată îmi dau un alt răspuns. De obicei au un singur răspuns: „Pentru că putem”. Şi eu le spun: „Bine, nu vă pun la îndoială autoritatea – de fapt, ba da, vă pun la îndoială autoritatea, doar că nu o fac acum –, vreau pur şi simplu să ştiu de ce mi se întâmplă lucrurile astea”. Acum mi se spune tot timpul: „Păi nu e evident? Lucrezi la Tor” sau „Stai pe scaunul de lângă

Julian, la ce te aşteptai?” Mi se pare fascinant că fiecare dintre cei care mă reţin – de regulă de la Serviciul Vamal şi de Protecţie a Frontierei sau de la Serviciul pentru Controlul Imigraţiei şi Normelor Vamale din Statele Unite – îmi spune că, mai mult decât orice, o fac din cauză că au autoritatea să o facă. Mi s-au spus şi rahaturi de genul „îţi aminteşti de 11 septembrie? De aia”, sau „Pentru că vrem să ne răspunzi la nişte întrebări, iar ăsta este locul în care ai cele mai puţine drepturi, sau cel puţin aşa spunem noi”.

Iar în situaţii de genul acesta îţi vor refuza accesul la un avocat, îţi vor refuza accesul la o toaletă, dar îţi vor da apă, îţi vor da ceva de băut, un diuretic, de exemplu, pentru a te convinge că e în interesul tău să cooperezi în vreun fel. Au făcut acestea pentru a mă presa, din motive politice. Mi-au pus întrebări despre părerea mea în legătură cu războiul din Irak, despre părerea mea în legătură cu războiul din Afghanistan. Practic, au repetat tacticile folosite de FBI în timpul operaţiunii COINTELPRO (uriaşul program de operaţiuni domestice sub acoperire care a fost în funcţiune între 1956 şi 1971). De pildă, au încercat în mod direct să-şi afirme autoritatea de a schimba realităţi de ordin politic din viaţa mea şi de a încerca să mă preseze nu doar să le schimb, ci să le acord un soi de cale specială de acces la ceea ce se petrece în capul meu. Şi mi-au confiscat lucruri aflate în proprietate. Nu prea sunt autorizat să vorbesc despre toate lucrurile care mi s-au întâmplat pentru că este o zonă gri şi foarte obscură şi nici nu ştiu exact dacă mi-e permis măcar să vorbesc în general despre ele. Sunt sigur că s-au întâmplat şi altor oameni, doar că eu nu am auzit niciodată să li se fi întâmplat.

Eram odată la aeroportul Pearson din Toronto, mă întorceam acasă de la o întâlnire cu familia. Călătoream

spre Seattle, unde locuiam în acea vreme, şi m-au reţinut, m-au dus la un control de securitate secundar, apoi la un control de securitate terţiar, iar într-un final într-o celulă de detenţie. Şi m-au ţinut acolo atât de mult, încât când într-un final mi-au dat drumul, am ratat zborul. Dar lucrul curios este că aceste zone de predetenţie sunt de fapt teritoriu american pe teritoriul canadian, aşa că au o regulă conform căreia, dacă ţi-ai ratat zborul sau dacă mai e foarte mult până la următorul zbor, eşti obligat să pleci. Deci am fost de fapt dat afară din America din cauză că am fost reţinut atât de mult şi a trebuit să intru în Canada, să zbor în altă parte a ţării, să-mi închiriez o maşină, apoi să trec frontiera cu maşina. Şi când am ajuns la frontieră mi-au spus: „Cât timp aţi petrecut în Canada?”, iar eu le-am spus „Păi, cinci ore plus reţinerea din Toronto”, deci fusesem în Canada vreo opt ore, şi mi-au spus „Intraţi, şi vă vom reţine din nou”. Apoi mi-au făcut maşina bucăţi, mi-au dezmembrat laptopul, s-au uitat prin toate aceste lucruri, după care m-au reţinut. Mi-au permis accesul la o toaletă după o jumătate de oră, s-ar putea spune că au fost foarte milostivi. Iar asta este ceea ce ei numesc percheziţia vamală de excepţie – genul acesta de comportament are loc pentru că au capacitatea, spun ei, să o facă, şi nimeni nu le poate imputa nimic în legătură cu asta.100

JULIAN: Aşadar, acestea ţi s-au întâmplat ţie, dar persoanele din China cu care vorbesc, când îmi spun despre marele firewall al Chinei – în Occident vorbim în principal despre asta în termeni de cenzură, despre faptul că cetăţenii Chinei sunt împiedicaţi să iasă şi să citească ce se spune despre guvernul chinez în Occident, de către disidenţi chinezi, de către Falun Gong şi de către BBC şi, s-o recunoaştem, în însăşi propaganda despre China –, dar îngrijorarea lor nu este de fapt legată de cenzură. Ceea ce-

i îngrijorează este că pentru cenzurarea internetului e nevoie şi de supravegherea sa. Pentru a verifica ce pagini accesează cineva, pentru a vedea dacă acestea sunt permise sau restricţionate, trebuie să le poţi vedea, iar dacă le vezi înseamnă că le poţi şi arhiva. Iar lucrul acesta a avut efectul de a înspăimânta populaţia Chinei – nu faptul că sunt supuşi cenzurii, ci faptul că tot ceea ce citesc este spionat şi înregistrat. În realitate, lucrul acesta este adevărat şi pentru noi. Acesta e un lucru care schimbă oamenii, în momentul când îl conştientizează. Le modifică comportamentul, iar ei devin mai puţin fermi în nemulţumirea faţă de diferite autorităţi.

JACOB: Aceasta este totuşi o reacţie greşită la genul acela de influenţă. Hărţuirea pe care am suferit-o la frontiere, de exemplu, nu e unică, în sensul că, după şi chiar înainte de 11 septembrie, fiecare cetăţean american de origine arabă a trebuit să treacă prin aşa ceva. Doar că eu refuz să-mi irosesc privilegiul de a avea pielea albă şi paşaport SUA şi refuz să tac în legătură cu asta, pentru că lucrurile pe care le fac aceste persoane nu sunt corecte şi pentru că abuzează de puterea pe care o folosesc. Şi trebuie să ne opunem acestor lucruri, la fel cum există şi în China persoane curajoase care se opun, cum ar fi Isaac Mao, de pildă.101 El s-a opus foarte vehement, şi în mod eficient, acestui gen de cenzură, pentru că reacţia adecvată nu este pur şi simplu să cedezi în faţa acestui tip de presiune doar din cauză că guvernul afirmă că are puterea să o facă.

JÉRÉMIE: Dar aici vorbim din nou despre politică, pentru că ceea ce spui tu este, în esenţă, că oamenii ar trebui să lupte pentru drepturile lor – dar oamenii ar trebui să înţeleagă de ce trebuie să o facă, iar apoi ar trebui să aibă capacitatea de a comunica unii cu alţii

pentru a o face. Am avut ocazia să vorbesc cu unele persoane din China – şi nu ştiu dacă ocupau vreo poziţie în stat sau dacă au fost selectate pentru a putea să iasă şi să vorbească cu mine –, dar când i-am întrebat despre cenzura internetului, am primit foarte des acest răspuns: „Păi, este pentru binele Poporului. Există cenzură, sigur, pentru că dacă nu ar fi existat cenzură ar fi existat comportamente extremiste, ar fi existat lucruri neplăcute pentru toată lumea, iar guvernul ia aceste măsuri pentru a se asigura că totul merge bine”.

JACOB: Este acelaşi argument precum cel pentru prelevarea de organe. Nu faceţi risipă de organe!

JÉRÉMIE: Dacă ar fi să ne uităm la modul în care este implementată cenzura în China, am vedea că, din punct de vedere tehnic, este unul dintre cele mai avansate sisteme din lume.

JACOB: Foarte adevărat.

JÉRÉMIE: Şi am auzit că pe Weibo – care este echivalentul chinezesc al Twitterului – guvernul poate filtra unele *hashtags* pentru a se asigura că ele nu părăsesc o anumită provincie.

JACOB: Este esenţial să nu pierdem din vedere faptul că atunci când se vorbeşte despre cenzura din Asia, ne place să vorbim în termeni de „celălalt” – de parcă afectează doar oamenii din „X-istan”. Este foarte important să se ştie că atunci când cauţi pe Google în Statele Unite, îţi spun că au omis unele rezultate din considerente legale. Există o diferenţă între cele două – atât la nivelul modului în care sunt implementate, cât şi, evident, la nivel de realitate socială a lui cum, al lui de ce, chiar şi a lui unde privitor la cenzură – dar o mare parte a diferenţei ţine de arhitectură. De exemplu, asupra internetului american, fiind foarte descentralizat, este foarte greu să

implementezi o cenzură după modelul Chinei.

JULIAN: Ei bine, o mare parte a sa e reprezentată de Google, iar Google poate fi cenzurat. Există o grămadă de pagini care fac referire la Wikileaks şi care sunt cenzurate de Google.

JACOB: Da, fără îndoială. Şi, de fapt, pentru că indexul ca atare este liber, se poate face o analiză diferenţială.

JULIAN: Da, teoretic.

JACOB: Teoretic. Iar practic, există nişte persoane care lucrează la genul acesta de detector de cenzură uitându-se la diferenţele văzute din diferite perspective din lume. Cred că este important să ne amintim că cenzura şi supravegherea nu sunt probleme din „alte locuri” – occidentalilor le place să vorbească despre cum „oamenii din Iran, China şi Coreea de Nord au nevoie de anonimitate şi libertate, dar aici nu avem nevoie de ele”. Şi când spun „aici” vor de regulă să spună „în Statele Unite”. Dar de fapt nu e vorba doar de regimuri politice opresive, fiindcă dacă se întâmplă să faci parte din eşalonul de top al oricărui regim, pentru tine nu va fi opresiv. Dar avem impresia că Regatul Unit este un loc minunat; de regulă se crede că Suedia ar fi o ţară splendidă, şi totuşi putem vedea că atunci când ieşi din graţiile celor aflaţi la putere, nu ajungi într-o poziţie favorabilă. Dar Julian este încă în viaţă, nu-i aşa? Deci e clar că acesta este un semn că avem de-a face cu o ţară liberă – am dreptate?

JULIAN: Am muncit mult pentru a-mi menţine poziţia pe care o am acum. Dar poate că ar trebui să vorbim despre cenzura internetului în Occident. Este un lucru foarte interesant. Dacă ne întoarcem în anul 1953 şi ne uităm la marea Enciclopedie sovietică, care a fost distribuită peste tot, vedem că ea a suferit modificări de

fiecare dată când au existat schimbări de ordin politic în Uniunea Sovietică. În anul 1953 a murit Beria, şeful NKVD-ului, poliţia secretă sovietică, şi a ieşit din favorurile politice, astfel că secţiunea sa, care-l descria în termeni strălucitori, a fost tăiată de către autorităţile care se ocupau de enciclopedie, care au emis un amendament ce trebuia introdus în toate aceste enciclopedii. Era extrem de evident. Menţionez acest exemplu din cauză că era atât de evident şi putea fi detectat atât de uşor încât încercarea aceasta a devenit istorică. În timp ce în Regatul Unit avem *The Guardian* şi alte ziare importante care scot în secret articole din arhivele lor online fără niciun fel de explicaţii. Dacă aţi accesa paginile acestea acum şi aţi încerca să le găsiţi, de exemplu articole despre cazul de fraudă al miliardarului Nadhmi Auchi, aţi primi rezultatul „Page Not Found", şi au fost scoase şi din indexuri.

Să vă povestesc despre implicarea mea în povestea lui Nadhmi Auchi. În anul 1990, Irakul a invadat Kuwaitul, iar asta a dus la primul Război din Golf. Guvernul Kuwaitului a avut nevoie de bani în timpul exilului, dar şi după reîntoarcerea în ţară, aşa că a început să scoată la vânzare mai multe bunuri, inclusiv câteva rafinării de petrol din afara graniţelor ţării. Un afacerist englez.

Nadhmi Auchi, care imigrase în anii '80 în Regatul Unit din Irak, unde fusese un personaj în regimul lui Saddam Hussein, a fost broker în acea vânzare şi a fost după aceea acuzat că ar fi fost implicat în transferul de comisioane ilegale în valoare de 118 milioane de dolari. Acea investigaţie a fost cea mai mare investigaţie de corupţie din istoria Europei de după război. În anul 2003, Nadhmi Auchi a fost declarat vinovat de fraudă în ceea ce a devenit cunoscut ca Scandalul Elf Aquitaine. Cu toate acestea, astăzi are peste 200 de companii înregistrate în

holdingul său din Luxemburg şi altele în Panamá. Este implicat într-o afacere de telefonie mobilă în Irak şi în multe alte afaceri pe glob.102

În Statele Unite, Tony Rezko, care a strâns fonduri pentru campania pentru Senat a lui Barack Obama, era un amic vechi de-al lui Auchi, acesta din urmă fiind în trecut finanţatorul său. De asemenea, Auchi şi Rezko s-au asociat cu fostul guvernator al statului Illinois, Rob Blagojevich. Atât Rezko, cât şi Blagojevich au fost găsiţi vinovaţi de corupţie, Rezko în 2008, iar Blagojevich în 2010/2011 (după ce FBI-ul i-a înregistrat un apel telefonic interceptat în care încerca să vândă fostul loc în Senat al lui Obama). În 2007/2008, când Obama era în campania pentru a fi ales candidatul partidului Democrat la alegerile prezidenţiale, presa din SUA a început să investigheze relaţiile lui Obama. L-au investigat pe Rezko şi au găsit nişte conexiuni relativ la cumpărarea casei lui Barack Obama. În 2008, cu puţin timp înaintea procesului său, Rezko a primit priii transfer 3, 5 milioane de dolari de la Auchi pe care nu i-a declarat Curţii, deşi era obligat să o facă – motiv pentru care a şi fost închis. Aşa că cercetările amănunţite ale presei din SUA s-au îndreptat către Auchi, iar în acel moment el a poruncit avocaţilor de la Carter-Ruck din Regatul Unit să înceapă o campanie agresivă împotriva unei mari părţi a reportajelor din 2003 despre scandalul Elf Aquitaine şi condamnarea sa în Franţa. Campania a avut un mare succes.

S-a îndreptat împotriva presei din Regatul Unit, dar şi împotriva unor bloguri din SUA şi a cerut scoaterea de pe internet a cel puţin 12 articole, din câte ştim noi. Majoritatea acelor articole, inclusiv cele din arhivele ziarelor din Regatul Unit, au dispărut, pur şi simplu. Era ca şi cum nici nu ar fi existat vreodată. Nu a existat niciun soi

de „Am primit o plângere de ordin juridic şi am decis să scoatem articolul”. Au dispărut şi din indexuri. Wikileaks le-a scos la iveală şi le-a publicat din nou.103

JACOB: Ei şterg istoria.

JULIAN: Istoria nu e doar modificată, ci a încetat să fi existat vreodată. Este dictonul lui Orwell: „Cel care controlează prezentul controlează trecutul, iar cel care controlează trecutul controlează viitorul”. Este ştergerea imposibil de detectat a istoriei în Occident, iar asta este doar cenzura de după publicare. Autocenzura dinaintea publicării este mult mai gravă, dar deseori greu de detectat. Am putut observa asta în cazul publicării Cablegate, pentru că Wikileaks lucrează cu mai mulţi parteneri media pe tot mapamondul, deci putem vedea care dintre ei cenzurează materialul nostru.104

De exemplu, publicaţia *New York Times* a cenzurat o telegramă care spunea că au fost distribuite milioane de dolari pentru influenţarea anumitor cetăţeni libieni cu legături politice, prin intermediul unor companii petroliere libiene. Telegrama nici măcar nu făcea referire la o anumită companie petrolieră – *New York Times* a editat pur şi simplu sintagma „companii petroliere”.105 Cel mai flagrant caz este probabil citarea de către *New York Times* a unei telegrame de şaizeci şi două de pagini despre programul de rachete al Coreei de Nord şi despre faptul dacă vânduseră sau nu rachete Iranului, telegramă din care *New York Times* s-a folosit de două paragrafe pentru a argumenta, într-un articol, teza că Iran ar avea rachete care ar putea lovi Europa, în timp ce în alte părţi ale telegramei se argumenta tocmai teza opusă.106

The Guardian a editat o telegramă despre Iulia Timoşenko, fostul prim-ministru al Ucrainei, în care se menţiona că şi-ar ascunde banii la Londra.107 A cenzurat

afirmaţiile, conform cărora elita Kazahstanului, în general, ar fi coruptă – nici măcar o persoană nu era numită – şi afirmaţia că ENI, compania energetică italiană cu sediul în Kazahstan, şi British Gas ar fi corupte.108 În esenţă, *The Guardian* a cenzurat cazurile în care o persoană bogată era acuzată de ceva, excepţie făcând situaţiile în care *The Guardian* avea ceva împotriva acelei persoane bogate.109 Astfel, de pildă, într-o telegramă despre organizaţiile criminale din Bulgaria apărea şi numele unui personaj rus, iar *The Guardian* a dat impresia că întreaga telegramă era despre el, dar el era doar un singur personaj într-o listă lungă de organizaţii şi persoane implicate în organizaţiile criminale ale Bulgariei.110 *Der Spiegel* a cenzurat un paragraf despre Angela Merkel – nu din pricina unor violări ale drepturilor sale, ci din simple raţiuni politice.111 Exemplele sunt multe.112

ANDY: Concepţia noastră despre libertatea informaţiei şi fluxul liber al informaţiei este într-un fel o concepţie nouă şi radicală, dacă ne uităm la întreaga planetă. Aş spune că nu e atât de diferită în Europa faţă de alte ţări. Da, există unele ţări care funcţionează după un model democratic, ceea ce înseamnă că poţi citi, poţi înţelege şi poate chiar ataca în instanţă infrastructura cenzurii, dar asta nu înseamnă că cenzura nu există acolo, în vreme ce în ţări ca Arabia Saudită sau China îţi va fi foarte greu să o faci.

JULIAN: Experienţa mea mi-a arătat că în Occident este doar mult mai sofisticată, prin caracterul vag şi straturile din ce în ce mai obscure în care este învelit tot ce se întâmplă. Aceste straturi există pentru ca cenzura să poată fi ascunsă, negată. Vă puteţi închipui procesul cenzurii ca pe o piramidă. Piramidei îi iese doar vârful din nisip, iar lucrul ăsta e intenţionat. Vârful este public –

cazurile de calomnie, asasinările jurnaliştilor, camerele de fotografiat smulse de personalul militar şi aşa mai departe –, cenzura cunoscută, publică. Dar acesta este elementul cel mai mic. Următorul strat de sub vârf este format din toate persoanele care nu-şi doresc să fie în vârf, care se autocenzurează pentru a nu ajunge acolo. Apoi, în următorul strat se află tot soiul de stimulente economice, sau stimulente sub forma patronajului care se oferă unor persoane pentru a scrie despre anumite subiecte. Următorul strat este economie pură – ce subiecte sunt avantajoase din punct de vedere economic, chiar şi fără includerea factorilor economici din straturile superioare ale piramidei. Mai departe, următorul strat este format din prejudecăţile cititorilor care au doar un anumit nivel de educaţie, deci care, pe de-o parte, pot fi manipulaţi uşor cu informaţii false, dar cărora, pe de altă parte, nici nu le poţi spune ceva adevărat şi prea sofisticat. Ultimul strat este distribuţia – bunăoară, unii oameni pur şi simplu nu au acces la informaţie într-o anumită limbă. Aşadar, aceasta este piramida cenzurii. Ceea ce face *The Guardian* cu redactările Cablegate se află în cel de-al doilea strat.

Acum, genul acesta de cenzură poate fi negată, fie din cauză că are loc în ascuns, fie din cauză că nu există nicio instrucţiune de a cenzura o anumită afirmaţie. Jurnaliştilor rareori li se spune: „Nu scrie nimic despre asta” sau: „Nu scoate la tipar informaţia aceea”. Mai degrabă e subînţeles că se aşteaptă de la ei să o facă, fiindcă înţeleg interesele celor cu care doresc să fie în relaţii bune sau de care doresc să se apropie. Dacă te porţi cum se cade vei fi mângâiat pe cap şi recompensat, iar dacă nu, nu vei fi recompensat. E cât se poate de simplu. Îmi place adeseori să dau exemplul acesta: cenzura pe faţă care se făcea în Uniunea Sovietică, cenzura despre care s-

a vorbit atât de mult în Occident – agresorii care veneau la miezul nopţii şi scoteau jurnaliştii din casele lor –, a fost decalată cu douăsprezece ore. Acum se aşteaptă lumina zilei pentru a se sechestra casele jurnaliştilor, atunci când aceştia îşi pierd protectorul şi nu-şi mai pot plăti datoriile. Jurnaliştii sunt scoşi afară din case, acestea fiindu-le luate. Societăţile occidentale s-au specializat în spălarea cenzurii şi în structurarea afacerilor celor puternici de aşa manieră încât orice discurs public rămas care reuşeşte să răzbească să fie prea slab pentru a afecta relaţiile de putere ale unei societăţi puternic fiscalizate, pentru că aceste relaţii sunt ascunse în straturi de complexitate şi secrete.

ANDY: Jérémie a spus ceva despre pedo-naziști.

JACOB: Iarăşi ne-am întors la pedo-naziști.

JÉRÉMIE: Doi călăreţi într-unul singur.

ANDY: Chestiunea pedo-naziştilor rezumă argumentele Germaniei, poate chiar ale unei părţi a Europei, în favoarea cenzurii. Germania nu-şi dorea niciun fel de discursuri de incitare la ură pe internet din cauza istoriei sale şi, desigur, dacă spui că e nevoie să restricţionezi internetul din cauza pedofililor, vei putea face orice. De asemenea, a existat o circulară internă în Comisia Europeană referitoare la chestiunea reţinerii de date care menţiona: „Ar trebui să discutăm mai des despre pornografia infantilă şi atunci oamenii vor fi de acord”.113

JULIAN: Poţi vorbi şi despre chestiunea asta puţin? Despre faptul că dacă vrem să cenzurăm un singur lucru, să spunèm doar pornografia infantilă, atunci, pentru a cenzura pornografia infantilă, pentru ca ea să nu mai poată fi văzută, trebuie să supraveghem totul şi pe toată lumea. E nevoie să construim infrastructura. Trebuie să construim un sistem de spionaj şi cenzură în masă pentru a cenzura

un singur lucru.

ANDY: Totul stă în detaliile mecanismului – aşa-numitul sistem de precenzură din Germania te obligă să numeşti persoana care e responsabilă din punct de vedere legal pentru ceea ce publici. Deci, în linii mari, dacă publici ceva, fie că e pe o foaie de hârtie sau pe internet, fără să spui cine e responsabilul legal pentru conţinut, ai încălcat deja legea. Asta înseamnă că aloci responsabilitatea, iar dacă cineva încalcă legea şi distribuie, să spunem, pornografie infantilă sau discursuri care incită la ură, poţi spune pur şi simplu „în regulă, ne uităm care este adresa individului, îl prindem şi scoatem lucrurile astea de pe internet”.

JULIAN: Adică îl cenzurăm pe cel care publică, nu pe cel care accesează.

ANDY: Da. Şi se urmăresc doar anumite lucruri. Sunt de acord că nu orice lucru trebuie să poată fi accesat oricând, pentru că dacă mă uit la problemele legate de discursurile de incitare la ură, găsesc câteodată lucruri cu adrese private ale unor persoane şi aşa mai departe, lucruri care pot duce la situaţii cu care nu sunt de acord.

JULIAN: Dar, Andy, e un lucru foarte nemţesc. Pentru a putea face asta, pentru a stabili ce este acceptabil şi ce nu, trebuie să existe o comisie, trebuie să numeşti persoane în acea comisie, trebuie să existe un întreg proces de numire în comisie…

ANDY: Da, avem toate rahaturile astea. Crimele Germaniei din cel de-al Doilea Război Mondial – pentru tot ceea ce au făcut naziştii, pentru fiecare proprietate pe care au sechestrat-o, au emis chitanţe, au făcut o listă. Totul era compus din acte birocratice. Poţi foarte bine să spui că Germania a ucis fără motiv o grămadă de oameni – şi este adevărat –, dar a făcut-o într-o manieră birocratică. Aşa e

Germania.

JULIAN: Ca cineva să decidă ce ar trebui cenzurat şi ce nu, ai nevoie de două lucruri. În primul rând, trebuie să construieşti infrastructura tehnică pentru a efectua cenzura. Trebuie să construieşti o maşinărie naţională de cenzură care să opereze eficient. Iar în al doilea rând, trebuie să ai o comisie şi un aparat birocratic. Iar acea comisie nu poate să fie decât secretă, din cauză că întreaga maşinărie devine inutilă în cazul în care nu e secretă, şi atunci ai justiţie secretă.

ANDY: Ştii ceva? Avem un principiu bun în Germania.

JACOB: Unul singur?

ANDY: Principiul este că dacă nu e realistic ca o anumită lege să fie aplicată, atunci ea nu ar trebui să existe. Dacă o lege nu are noimă, bunăoară dacă interzici morile de vânt sau mai ştiu eu ce, atunci spunem „Haideţi, fiţi serioşi, lăsaţi-o baltă”. Noi, cei de aici, suntem inspiraţi de internetul pe care îl ştiam noi când se maturiza, de fluxul liber al informaţiilor, liber în sensul de nelimitat, neîngrădit, necenzurat, nefiltrat. Iar dacă aplicăm planetei Terra ceea ce înţelegem noi prin flux liber al informaţiilor – şi a fost aplicat, în mare măsură, întregii planete – vedem, desigur, că guvernele au fost afectate de lucrul acesta şi vedem modul în care a fost aplicată puterea şi modul în care a fost gestionată cenzura, fie că e precenzură, posteenzură sau ce ştiu eu ce fel de cenzură. Cu toţii am aflat despre complicatele conflicte care apar. Întrebarea importantă este care e concepţia noastră despre guvern sau despre viitorul unei Organizaţii Post-Guvernamentale – poate Wiki-Leaks este prima sau una dintre primele OPG-uri –, pentru că nu sunt sigur că guvernele sunt răspunsul corect la toate problemele acestei planete, cum ar fi cele legate de mediu.

JULIAN: Nici guvernele nu ştiu sigur care este hotarul între ce ţine de guvern şi ce nu. E un hotar neclar. Guvernele ocupă spaţiu, dar Wikileaks ocupă o parte din spaţiul internetului. Spaţiul internetului este încorporat în spaţiul real, dar, din pricina gradului de complexitate dintre obiectul încorporat şi încorporarea ca atare, nu este uşor, din perspectiva încorporării, să determinăm că obiectul este încorporat. Din acest motiv avem sentimentul acesta al ciberspaţiului – că ar fi de fapt un alt tărâm care există pe undeva –, din cauza caracterului său indirect, complex şi universal. Când citiţi un fişier de pe internet într-o anumită locaţie este la fel ca a-l citi într-o altă locaţie sau în viitor – aceasta este universalitatea sa. Deci în sensul acesta, ca organizaţie care ocupă spaţiul cibernetic şi reuşeşte să transmită informaţii în spaţiul mai amplu în care e încorporat acesta, poate că suntem o organizaţie posistatală, din cauza lipsei controlului geografic.

Nu vreau să împing această analogie prea departe, din cauză că mă aflu sub arest la domiciliu. Este evident că forţa coercitivă a statelor se aplică tuturor oamenilor noştri, oriunde au fost identificaţi. Dar restului presei îi place să afirme că am fi o organizaţie media în afara oricărui stat şi are mare dreptate cu privire la importanţa neapartenenţei la vreun stat. Obişnuiam să spun mereu: „Ce credeţi voi că e Newscorp? O mare multinaţională”. Dar, în ciuda acestui lucru, Newscorp este structurată de aşa manieră încât se poate ajunge la componentele sale cheie, iar acesta este motivul pentru care a avut atât de mult de suferit aici, în Regatul Unit, în urma scandalului de hacking al telefoanelor, şi motivul pentru care încearcă acum să se dea atât de bine pe lângă administraţia SUA. Dar dacă activele unei organizaţii sunt în primul rând informaţiile pe care le deţine, atunci ea poate depăşi

graniţele naţionale într-un fel care este destul de greu de împiedicat, ca rezultat al criptografiei. Există un motiv bine întemeiat pentru care s-a ridicat o blocadă financiară împotriva noastră – celelalte elemente ale organizaţiei noastre sunt mult mai greu de eliminat.114

JACOB: Dacă e să vorbim despre asta în termeni utopici, ar trebui să ne întoarcem în timp puţin mai mult. Aşadar, m-ai întrebat despre hărţuirea la care am fost supus, m-ai întrebat despre cenzura din Occident şi am vorbit mai devreme despre programul de asasinări la comandă al lui Obama, despre care se afirmă că ar fi legitim din cauză că e la mijloc un proces, deci e considerat un proces echitabil.

JULIAN: Ei bine, un proces secret.

JACOB: Putem să ne întoarcem în timp şi să legăm chestiunea asta şi de John Gilmore. Unul dintre procesele intentate de John Gilmore în legătură cu dreptul său de a călători în anonimat în Statele Unite s-a încheiat când Curtea a spus literalmente: „Uite, o să consultăm legea, care e secretă. O vom citi şi vom afla, citind această lege secretă, dacă ai voie să faci lucrul pe care ai voie să-l faci”. Şi au descoperit, după ce au citit legea secretă, că, de fapt, avea voie să-l facă, fiindcă ceea ce spunea legea secretă nu-i limita libertatea. Nu a aflat niciodată ce stipula legea secretă, iar mai târziu au schimbat *politicile* Administraţiei pentru Securitatea Transporturilor şi ale Departamentului de Securitate Internă al SUA, ca reacţie la victoria sa în acest proces, pentru că se pare că legea secretă nu era destul de restrictivă.115

JULIAN: Aşa că au făcut-o şi mai restrictivă?

JACOB: Practic, da, permiţând legiferarea birocraţiei. Dar este important să atragem atenţia că programul asasinărilor la comandă, hărţuirea pe care o au de

înfruntat oamenii la frontiere, cenzura online, cenzura pe care o implementează corporaţiile la porunca vreunui guvern sau la porunca vreunei corporaţii, toate aceste lucruri sunt legate unele de altele. Şi totul se rezumă la faptul că statul are prea multă putere în fiecare din locurile în care vedem că apar aceste fenomene. Aceasta se întâmplă din cauză că puterea s-a concentrat în aceste zone şi a atras persoane care abuzează de ea sau care fac presiuni pentru a se recurge la ea. Şi chiar dacă se întâmplă câteodată să existe cazuri legitime, ceea ce se poate observa este că lumea ar fi mult mai bună dacă nu ar exista această centralizare, dacă nu ar exista tendinţa către autoritarism.

Occidentul nu este deloc un caz special în acest sens, pentru că se pare că dacă ai un ţar al securităţii cibernetice, situaţia nu este atât de diferită faţă de cea a altor naţiuni de acum cincizeci de ani, în care aveai un ţar al forţelor de securitate internă. Construim acelaşi gen de structuri autoritare de control, care vor atrage persoane care vor abuza de ele, iar acesta este un lucru despre care ne place să pretindem că ar fi altfel în Occident. Nu este altfel în Occident, pentru că există un continuum al guvernării, de la autoritarism la libertarianism. Nu o spun în sensul partidelor politice americane, ci în acest sens: pe linia acelui continuum, Statele Unite sunt foarte departe de URSS în multe, multe aspecte, dar sunt mult mai aproape de URSS decât e Christiania, cartierul autonom din inima oraşului Copenhaga, în Danemarca.116 Şi este chiar mai departe, cred eu, de o lume potenţial utopică pe care am crea-o dacă am coloniza planeta Marte. Am vrea să îndepărtăm cât se poate de mult de totalitarism şi de autoritarism ceea ce am putea construi pe Marte. Câtă vreme nu avem aşa ceva, ceea ce avem sunt eşecuri.

JÉRÉMIE: Din nou, toate acestea sunt legate între ele. Când vorbim despre concentrarea puterii vorbim din nou despre arhitectură. Iar când vorbim despre cenzura internetului, este vorba despre centralizarea puterii de a determina ce se poate accesa şi ce nu, şi dacă cenzura guvernamentală, sau chiar cenzura privată, este sau nu o putere necuvenită. Avem acest exemplu: site-ul nostru, *laquadrature.net*, a fost cenzurat în Regatul Unit de către Orange UK timp de câteva săptămâni. Se afla într-o listă de site-uri a căror accesare era interzisă de către Orange celor care au mai puţin de optsprezece ani. Poate că am menţionat termenul de pornografie infantilă când ne-am opus tipului acestuia de legislaţie, sau poate că pur şi simplu nu le plăcea de noi din cauză că ne opunem politicii lor împotriva neutralităţii internetului, deoarece noi militäm pentru o lege care să le interzică să discrimineze comunicaţiile utilizatorilor lor.117 Nu vom afla niciodată. Dar iată un actor privat care, sub formă de serviciu, se oferă să le ia oamenilor posibilitatea de a accesa anumite informaţii pe internet. Eu văd aici un risc major, în spatele puterii pe care o dăm, fie companiei Orange, fie guvernului Chinei sau mai ştiu eu cui.

JACOB: Să clarificăm ceva – când spui privat în Regatul Unit, vrei să spui că deţin fiecare linie, fiecare conexiune cu fibră optică şi tot, sau folosesc şi din resursele statului? Cum au fost autorizate oficial undele radio? Statul nu intervine deloc? Nu au o obligaţie să fie vigilenţi[6]?

JÉRÉMIE: Există autorizare. Se schimbă arhitectura

6 In original, duty of care, termen juridic care indică obligaţia individului sau a unei organizaţii de a respecta un standard rezonabil de vigilenţă în timpul săvârşirii unor acţiuni care ar putea dăuna altor indivizi sau organizaţii, (n.tr.)

internetului, are loc o trecere de la o singură reţea universală la divizarea într-o serie de subreţele mici. Dar ceea ce discutăm noi de la început sunt probleme globale, fie că vorbim despre declinul sistemului financiar, fie că vorbim despre corupţie, fie că vorbim despre geopolitică sau despre problema energetică sau despre mediu. Toate acestea sunt problemele globale cu care se confruntă omenirea în zilele noastre şi încă avem un instrument în mâinile noastre, unul global, care ne permite să comunicăm mai bine, să răspândim cunoaşterea mai bine, să participăm mai bine la procesele politice şi democratice. Ceea ce tind eu să cred este că un internet global, universal, este singurul instrument cu care am putea să abordăm aceste probleme globale, iar acesta este motivul pentru care această bătălie pentru libertatea internetului este bătălia cea mai importantă, cea în care avem cu toţii responsabilitatea să luptăm.

ANDY: Sunt totalmente de acord că trebuie să ne asigurăm că internetul este înţeles ca o reţea universală caracterizată printr-un flux liber de informaţie; trebuie nu doar să definim lucrul acesta foarte limpede, ci şi să dezvăluim numele acelor companii şi acelor furnizori de servicii care furnizează ceva ce ei numesc internet, dar care de fapt este ceva complet diferit. Dar cred că încă nu am răspuns la întrebarea-cheie dincolo de această chestiune a filtrării. Vreau să vă dau un exemplu referitor la chestiunea la care cred că e nevoie să răspundem. Cu câţiva ani în urmă, acum vreo zece ani, am protestat împotriva introducerii pe piaţă de către Siemens a unor aşa-numite software-uri pentru filtru smart. Siemens este una dintre cele mai mari companii de telecomunicaţii din Germania şi furnizor de echipamente de spionaj. Şi au vândut acest sistem de filtrare unor companii, astfel încât,

de pildă, angajaţii să nu se poată uita pe site-urile sindicatelor pentru a se informa despre drepturile lor şi aşa mai departe. Dar au blocat şi site-ul Clubului Chaos Computer, lucru care ne-a supărat. L-au desemnat ca având „conţinut criminal” sau ceva de genul, lucru pentru care am intentat acţiuni în instanţă. Dar la un târg am decis să organizăm un protest uriaş şi să înconjurăm standul Siemens şi să filtrăm oamenii care intră şi ies. Dar chestia amuzantă era că am anunţat protestul pe site-ul nostru pentru a atrage cât mai mulţi oameni prin internet, iar oamenii din standul Siemens habar n-aveau, pentru că şi ei foloseau software-ul de filtrare, aşa că nu putuseră să citească avertismentul care era afişat acolo la vedere.

JULIAN: Pentagonul a instalat un sistem de filtrare, astfel încât orice e-mail trimis către Pentagon care conţinea cuvântul Wikileaks să fie filtrat. Şi astfel, în cazul lui Bradley Manning, organele procuraturii au comunicat în timpul urmăririi penale cu persoane din afara armatei despre „Wikileaks”, dar nu au văzut niciodată răspunsurile primite, din cauză că ele conţineau cuvântul „WÂkileaks”.118 Statul siguranţei naţionale ar putea să-şi vină singur de hac.

AN DY: Ajungem astfel înapoi la întrebarea de bază: există ceva ce ar putea fi numit informaţie cu efect negativ? Adică, din punctul de vedere al societăţii, vrem să avem un internet cenzurat pentru că este mai bun pentru societate sau nu? Şi chiar dacă am vorbi despre pornografia infantilă ai putea spune: „Stai puţin, pornografia infantilă evidenţiază o problemă, şi anume abuzul copiilor, iar pentru a putea rezolva problema trebuie să cunoaştem problema”.

JACOB: Aşadar oferă dovezi ale infracţiunii.

JULIAN: Păi nu, oferă un lobby.

ANDY: Aceasta ar fi abordarea cea mai radicală, dar dacă vorbim despre naziști sau mai ştiu eu ce, trebuie totuşi să poţi spune despre ce vorbim. Persoanele care au familie se vor întreba: „Păi nu ar fi mai bine ca societatea să filtreze lucrurile negative, astfel încât să rămânem cu cele pozitive, sau nu cumva lucrul acesta ne-ar limita capacitatea de a vedea problemele şi de a le gestiona şi de a le trata şi de a le rezolva?”

JÉRÉMIE: Eu cred că tot timpul soluţia este alta decât cenzura. Când vorbim despre pornografia infantilă nu ar trebui nici măcar să folosim cuvântul pornografic – este reprezentarea unor scene infracţionale de abuz al copiilor. Lucrul care trebuie făcut este să mergem la servere, să le scoatem din funcţiune, să identificăm persoanele care au urcat conţinutul pe internet, pentru a identifica persoanele care l-au produs, acestea fiind cele care au abuzat copii. Iar de fiecare dată când există o reţea de oameni, o reţea comercială şi aşa mai departe, să arestăm acei oameni. Iar când adoptăm legi – şi avem una în Franţa care stipulează că o autoritate administrativă a Ministerului Afacerilor Interne decide care site-uri vor fi blocate – vom suprima orice interes al serviciilor de investigaţii de a găsi persoanele care fac ticăloşiile acestea, fiindcă spunem: „Oh, eliminăm pur şi simplu accesul la conţinutul negativ”, şi e ca şi cum am pune palma în faţa ochilor cuiva care observă o problemă şi am pretinde că am rezolvat-o. Deci, doar din acea perspectivă, cred că e de ajuns să descriem astfel lucrurile – în condiţiile în care suntem cu toţii de acord că ar trebui să eliminăm imaginile acelea de pe internet.

JACOB: Îmi pare rău, dar nu-mi găsesc deloc astâmpărul. Este foarte frustrant să ascult argumentul pe care îl susţii. Îmi vine să vărs, fiindcă ceea ce tocmai ai

făcut a fost să spui: „Vreau să-mi folosesc poziţia de putere pentru a-mi impune autoritatea asupra altor persoane, vreau să şterg istoria”. Poate că sunt un extremist în acest caz – şi în multe alte cazuri, sunt sigur –, dar am să fac nişte afirmaţii îndrăzneţe. Acesta este, de fapt, un exemplu de deserviciu făcut prin ştergerea istoriei. Am aflat, mulţumită internetului, că există în societate o epidemie a abuzării copiilor. Asta e ceea ce am aflat ca urmare a acestei probleme a pornografiei infantile – şi cred că ar fi mai bine să o numim exploatare infantilă –, am văzut dovezile acestui fapt. Cred că ascunderea şi eliminarea conţinutului sunt o bătaie de joc, pentru că, de fapt, poţi afla foarte multe despre societate în întregul ei. De pildă, poţi afla – şi e clar că nu voi avea niciodată o carieră în politică după ce termin propoziţia aceasta, dar trebuie să clarificăm chestiunea afli, de exemplu, cine sunt cei care produc acest conţinut, şi afli despre persoanele care le-au căzut victime. E imposibil ca oamenii să ignore problema. Înseamnă că trebuie să începi să cauţi cauza care dă naştere acestui lucru, adică pe cei care exploatează copiii. Printr-o ironie, cred că unele tehnologii de supraveghere ar fi utile aici, pentru recunoaşterea facială a celor implicaţi şi pentru a urmări metadatele imaginilor. Dacă am elimina conţinuturile acestea, asigurându-ne că trăim într-o lume în care e posibil să se şteargă unele lucruri şi alte lucruri nu, creând aceste corpuri administrative însărcinate cu cenzura şi cu elaborarea politicilor, am porni pe o pantă alunecoasă care, după cum am văzut, s-a îndreptat direct către drepturile de autor, şi s-a îndreptat către multe alte sisteme.

Poate nu ar trebui să alegem calea cea mai uşoară doar pentru că este o cauză nobilă să vânăm aceste înregistrări, poate ar trebui, de fapt, să încercăm să găsim

făptaşii crimelor, poate ar trebui de fapt să încercăm să-i ajutăm pe cei care au fost victimizaţi, chiar dacă genul acesta de ajutor costă. Poate, în loc să ignorăm problema, ar trebui să privim în faţă faptul că societatea, în întregul său, are această mare problemă care se manifestă pe internet într-un mod anume.

E ca atunci când, de exemplu, Polaroid a scos pe piaţă camera Swinger (camera care făcea fotografii instant), iar oamenii au început să facă fotografii abuzive şi cu aceste camere. Dar soluţia nu este să distrugem un anumit mijloc sau să-l supunem unui control poliţienesc. Soluţia este să găsim dovezi pentru a urmări în instanţă infracţiunile pe care acel mijloc le-a dezvăluit. Nu trebuie să şubrezim acel mijloc sau să mutilăm întreaga societate din cauza acestui lucru. Pentru că vorbim aici despre pornografia infanţilă, hai să vorbim despre poliţie. Poliţia abuzează oamenii în mod regulat într-o mulţime de ţări. Probabil sunt mai mulţi poliţişti abuzivi pe internet decât distribuitori de pornografie infantilă.

JULIAN: Aproape sigur sunt mai mulţi.

JACOB: Ştim că există un număr „na de poliţişti în lume şi ştim că un număr „xa dintre aceştia au comis încălcări de ordin etic – de regulă violente. Dacă ne uităm, de pildă, doar la mişcarea *Occupy*, vedem acest lucru. Ar trebui oare să cenzurăm internetul din cauză că ştim că unii poliţişti sunt ticăloşi? Ar trebui să mutilăm capacitatea poliţiei de a face bine?

JULIAN: Mai există şi chestiunea revictimizării, care se întâmplă când, mai târziu, copilul, sau adultul, sau persoanele cu care e el în contact social văd imaginile din nou abuzului.

JACOB: Atât timp cât acei poliţişti sunt online, sunt revictimizat.

JULIAN: Da, poţi spune că a vedea o imagine în care eşti bătut de un poliţist este revictimizare. Eu aş susţine că protejarea integrităţii arhivei istorice a lucrurilor care s-au întâmplat în lume este mai importantă; revictimizarea are loc, dar, oricum, instaurarea unui regim de cenzură capabil să elimine bucăţi de istorie ar însemna să nu putem aborda problema din cauză că nu o putem vedea. În anii ’90 am lucrat în calitate de consilier pe chestiuni legate de internet pentru nişte poliţişti însărcinaţi cu prinderea pedofililor în Australia, Unitatea Victoriană pentru Exploatarea Copiilor. Aceşti poliţişti nu se bucurau de introducerea sistemelor de filtrare, din cauză că atunci când oamenii nu pot vedea că există pornografie infantilă pe internet, se elimină lobby-ul care asigură poliţiştilor fondurile pentru a opri abuzul copiilor.

JEREMIE: Lucrul cu care suntem cu toţii de acord – şi care cred că este cel mai important – este că până la urmă cea care contează cu adevărat şi cea spre care poliţia ar trebui să-şi îndrepte atenţia este responsabilitatea individuală a persoanelor care produc conţinutul, materiale despre abuzul copiilor şi lucruri de genul acesta.

JACOB: Nu suntem de acord. Nu asta am spus.

JULIAN: Nu, Jérémie vorbeşte despre producere, nu despre publicare – e o diferenţă.

JACOB: Nu producerea conţinutului este problema, de fapt. Aş vrea să fac doar o mică clarificare – dacă, de exemplu, ai abuzat de un copil şi Andy a făcut o poză ca dovadă, nu cred că Andy ar trebui urmărit în instanţă.

JÉRÉMIE: Nu, e vorba de cei care fac abuzul. Să fim serioşi, e complicitate.

ANDY: Dar unii oameni abuzează de copil pentru a produce imaginile, nu-i aşa?

JACOB: Bineînţeles.

ANDY: S-ar putea să existe şi un aspect economic în chestiunea asta.

JACOB: Sunt în întregime de acord cu tine. Eu fac aici o distincţie, şi anume că dacă conţinutul ca atare este o probă istorică şi o dovadă a unei infracţiuni, este dovada unei infracţiuni foarte serioase, şi nu ar trebui să pierdem niciodată din vedere faptul că există fenomenul revictimizării, dar prima victimizare este problema fundamentală, fie că există imagini ale ei sau nu.

JÉRÉMIE: Desigur. Asta vreau să spun.

JACOB: aproape irelevant dacă există sau nu imagini. Când există imagini, este foarte important să ne amintim că trebuie să avem în vedere ţelul principal, şi că scopul este să oprim răul, să oprim abuzul. Asta înseamnă, în mare parte, că trebuie să ne asigurăm că există dovezile şi că există un stimulent pentru cei care au instrumentele potrivite să descopere făptaşii acestor infracţiuni. Lucrul acesta este, cred eu, foarte important, iar oamenii pierd din vedere lucrul acesta fiindcă le este mai uşor să se prefacă că nu există, iar apoi să oprească imaginile şi să spună că asta a oprit abuzul. Şi nu e adevărat.

AN DY: Şi problema este că acum poate mulţi oameni vor prefera, evident, soluţia mai uşoară, din cauză că este foarte supărător să ne uităm la ceea ce se întâmplă cu adevărat în societate. Cred că ai o şansă să te ocupi de o problemă politică deoarece nu încerci să creezi o politică care să ignore problema sau care să o facă invizibilă. Într-o anumită privinţă, poate fi vorba de politică cibernetică, dar mai e vorba şi de modul în care o societate abordează problemele, şi am dubii mari că informaţiile ar putea să facă rău în mod direct. Ţine, desigur, de capacitatea de a filtra şi e de asemenea adevărat că nu vreau să văd toate

imaginile care există pe internet. Exită unele care mi se par cu adevărat dezgustătoare şi altele care îmi distrag atenţia, dar acelaşi lucru este adevărat şi despre oricare magazin video care pune la dispoziţie filme fictive şi urâte. Deci întrebarea este: sunt în stare să gestionez ceea ce văd şi ceea ce procesez şi ceea ce citesc? Aceasta este abordarea bazată pe filtrare. Wau Holland, fondatorul organizaţiei Chaos Computer Club, a spus ceva amuzant: „Ştii, filtrarea ar trebui făcută la nivelul utilizatorului final şi la nivelul dispozitivului final al utilizatorului final". 119

JULIAN: Deci filtrarea ar trebui făcută de oamenii care primesc informaţia.

ANDY: Ar trebui făcută aici. Aici! (Arătând spre capul lui.) JULIAN: În creier.

ANDY: În dispozitivul final al utilizatorului final, adică lucrul pe care-l ai între urechi. Acolo ar trebui să filtrezi şi nu ar trebui ca filtrarea să fie făcută de guvern în numele poporului. Dacă poporul nu vrea să vadă unele lucruri, ei bine, nu e nevoit să le vadă, iar în zilele noastre trebuie să filtrezi multe lucruri oricum.

Confidenţialitate pentru cei slabi, transparenţă pentru cei puternici

JULIAN: Andy, am vorbit recent cu preşedintele Tunisiei şi l-am întrebat ce se va întâmpla cu arhivele de informaţii adunate în timpul domniei dictatorului Ben Ali – echivalentul tunisian al arhivelor Stasi – şi a spus că, deşi acestea sunt foarte interesante, agenţiile de spionaj reprezintă o problemă, sunt periculoase şi va trebui să le scoată din funcţiune una câte una. Dar în privinţa arhivelor, a crezut că ar fi cel mai bine pentru coeziunea societăţii tunisiene ca acestea să rămână secrete, ca să nu existe învinuiri. Erai tânăr în timpul căderii agenţiei Stasi în Germania de Est, poţi vorbi puţin despre arhivele Stasi

şi despre ceea ce crezi tu în legătură cu dezvăluirea arhivelor de securitate?

ANDY: Germania are probabil cea mai bine documentată agenţie de spionaj de pe planetă, sau cel puţin una dintre ele. Toate documentele provenind de la *Staatssicherheit*ul Germaniei de Est – fiecare manual, document de procedură, document de antrenament, studiu intern – sunt în cea mai mare parte publice, „în cea mai mare parte” înseamnă că nu toate pot fi accesate uşor, dar multe dintre ele pot, iar guvernul german a creat o agenţie care să se ocupe de arhive astfel încât cetăţenii Germaniei să aibă dreptul să-şi vadă dosarele Stasi.

JULIAN: Guvernul german a creat agenţi BStU (die Bundesbeauftragte für die Stasi-unterlagen), un mare distribuitor de dosare Stasi.

ANDY: Da, iar jurnaliştii pot aplica aşa-numitele anchete de cercetare, care sunt probabil comparabile cu cererile de acces la informaţie [în concordanţă cu Legea libertăţii informaţiei], care le permit să studieze dosarele. Şi există multe cărţi şi chiar manuale de comportament strategic ce arată felul în care Stasi făcea diverse lucruri. Cred, de fapt, că acesta este un lucru foarte bun de la care să putem învăţa. Înţeleg că e un pic prea mult să ne aşteptăm de la guvernul Tunisiei să publice toate dosarele personale alcătuite de fosta agenţie de spionaj din cauză că preşedintele – actualul preşedinte – va trebui să se gândească la propriile sale dosare, şi la cele ale aliaţilor săi şi aşa mai departe. Aceste agenţii de informaţii nu respectă confidenţialitatea, aşa că poţi avea dosare despre activităţile tale sexuale, telecomunicaţiile tale, transferurile de bani, despre tot ceea ce ai făcut vreodată, lucruri care poate nu vrei să fie dezvăluite.

J U LI AN: Ai urmărit situaţia cu Amn El Dawla,

securitatea de stat din Egipt? Mii de oameni au intrat şi au prădat arhivele în timp ce Amn El Dawla încerca să le ardă şi să le distrugă şi să le arunce la gunoi, şi multe dosare au ieşit şi au fost împrăştiate peste tot. Puteai cumpăra un dosar la piaţă cu 2 dolari şi să-l urci pe internet. Lucrul ăsta nu a distrus societatea egipteană.

ANDY: Nu, tot ceea ce spun eu este că înţeleg oarecum de ce unii oameni nu vor ca dosarele lor să fie dezvăluite. Pot înţelege asta, dacă mă gândesc cum ar fi fost să trăiesc într-o ţară în care s-au păstrat despre mine informaţii timp de patruzeci de ani şi de fiecare dată când mergeam la toaletă se nota.

JULIAN: Dar există şi analiza cost-beneficiu, nu? în opinia mea, turnător odată, turnător pe veci.

ANDY: Da, dar argumentul eticii hacker, în esenţă, este să foloseşti informaţii publice şi să protejezi informaţii sau date private, şi cred cu adevărat că dacă militäm pentru confidenţialitate – şi avem motive foarte bune să o facem – nu ar trebui să spunem doar că există un echilibru al lucrurilor aici. Putem face distincţia. Nu trebuie să lăsăm totul pe mâna publicului.

JACOB: Dar păstrarea aceasta a secretului are un beneficiu care e asimetric. Hai să luăm o anumită distanţă. şi să privim obiectiv. În esenţă, porneşti de la o premisă complet falsă, şi anume de la ideea că datele sunt private atunci când sunt limitate, iar lucrul ăsta pur şi simplu nu este adevărat. De pildă, dacă în ţara mea un milion de oameni au autorizaţia să acceseze datele astea private…

JULIAN: 4, 3 milioane…

JACOB: Cum poţi numi datele acelea private? Problema este că nu sunt sută la sută secrete pentru toată lumea.

JULIAN: Sunt secrete pentru cei fără putere, deţinute

de cei puternici.

ANDY: Da, ai dreptate. Dar dacă ar fi să deschidem o întreagă arhivă...

JULIAN: S-a întâmplat în unele ţări europene.

ANDY: Nu, nu ştiu de nicio ţară în care să fi fost făcute publice toate dosarele.

JULIAN: Într-o măsură mai mare decât în Germania, s-a întâmplat în Polonia, de pildă.

AN DY: Se prea poate. Ce s-a întâmplat, de fapt, partea negativă a acordului pe care l-a făcut Germania, este că au folosit foşti ofiţeri ai Securităţii de Stat a Germaniei de Est pentru ca Stasi să administreze nu doar arhivele Stasi, ci şi o parte a aşa-numitei „Noi Germanii", fosta parte de est, acum unificată. Există o relatare interesantă despre o companie care a câştigat licitaţia publică pentru a curăţa clădirea în care erau păstrate arhivele. Compania a câştigat licitaţia doar pentru că a licitat cel mai puţin pentru acelaşi serviciu pentru care licitau şi celelalte companii. După şase ani, organizaţia care administra arhiva a observat că angajase pentru curăţarea arhivei o companie creată de fosta agenţie de spionaj a Germaniei de Est.

JÉRÉMIE: A fost o relatare despre asta şi pe Wikileaks. Am citit-o. A fost foarte bună.120

ANDY: Wikileaks a publicat ştirea exact despre asta, aşa că ai dreptate atunci când spui că odată ce arhivele sunt create şi sunt în mâinile unor ticăloşi, e greu să vrei confidenţialitate.

JULIAN: Totuşi putem aborda o problemă mai amplă. Interne tul a dus la o explozie a cantităţii de informaţie accesibilă publicului – este pur şi simplu extraordinar. Funcţia educativă este extraordinară. Pe de altă parte, oamenii vorbesc despre Wikileaks şi spun: „Uite, toate

informaţiile private ale guvernului sunt acum publice, guvernul nu mai poate ţine nimic secret”. Eu spun că e o prostie. Spun că Wikileaks e doar umbra unei umbre. În realitate, faptul că am produs peste un milion de cuvinte de informaţie şi le-am dăruit publicului este doar o funcţie a imensei explozii la nivelul cantităţii de materiale secrete care există. Şi, de fapt, grupările puternice au acum o cantitate atât de vastă de materiale secrete încât face ca acea cantitate disponibilă public să pară minusculă, iar publicaţiile Wikileaks sunt doar o fracţiune a acestui material deţinut de privaţi. Când priviţi echilibrul acesta dintre pe de-o parte, oamenii puternici care ştiu despre fiecare tranzacţie cu cardul de credit din lume, iar, pe de altă parte, oamenii care caută pe Google toate blogurile lumii şi comentariile altor oameni, cum îl vedeţi?

AN DY: Aş putea spune că este un lucru bun ca toate arhivele acestea să fie făcute accesibile, pentru că oamenii vor afla că dacă-şi folosesc cardul de credit vor lăsa o urmă. Unora dintre oameni, dacă încerci să le explici lucrurile astea, li se vor părea foarte greu de înţeles şi foarte abstracte. Le vor înţelege în momentul în care îşi vor citi dosarul.

JULIAN: Dacă deschizi arhiva contului tău de Facebook, care are 800 MB de informaţii despre tine.

ANDY: Ştiu că după căderea blocului estic, cancelarul german Helmut Kohl a vrut să unifice Germania, iar americanii i-au impus o condiţie în cadrul aşa-numitelor negocieri 2 + 4. Au spus că doreau ca telecomunicaţiile Germaniei să rămână sub controlul lor, sub supravegherea lor, iar Kohl a crezut că nu este un lucru important, din cauză că nu a înţeles ce înseamnă supravegherea telecomunicaţiilor. M-am întâlnit cu cineva din cabinetul său şi acesta mi-a spus că cei din cabinet erau foarte

nemulţumiţi de decizia asta şi într-un final au aranjat ca aproximativ 8.000 de pagini de transcrieri ale apelurilor sale telefonice făcute de Stasi să fie aduse în biroul său pe două cărucioare mici. Iar el a zis: „Hei, ce-i cu astea?” Şi i-au răspuns că „Acestea sunt apelurile dumneavoastră telefonice din ultimii zece ani, inclusiv cele cu amantele dumneavoastră, cu soţia dumneavoastră, cu secretara dumneavoastră şi aşa mai departe”. Aşa că l-au făcut să priceapă ce înseamnă interceptarea de telecomunicaţii. Şi, într-adevăr, aceste dosare ale securităţii chiar ajută oamenii să înţeleagă ce fac agenţiile de informaţii. Deci am putea milita pentru publicarea completă şi dacă ar fi să votăm chiar acum, nu sunt sigur că m-aş opune.

JULIAN: Nu aş vrea să vorbim atât de mult despre chestiunea asta, din cauză că există evident şi cazuri în care dacă investighezi mafia, ar trebui ca informaţiile să rămână secrete pe durata investigaţiei. Există şi circumstanţe când lucrul ăsta ar putea fi văzut ca fiind legitim. Nu vreau să spun că este legitim ca tactică; vreau să spun că este inevitabil din punct de vedere politic. Există unele cereri atât de convingătoare din punct de vedere politic în favoarea sa – cum ar fi că „tipii ăştia au mai omorât şi înainte, acum pun la cale o altă crimă” –, încât indiferent dacă crezi sau nu că interceptările ar trebui să existe, ele vor exista oricum. Nu poţi câştiga bătălia asta politică. Dar acest tip de supraveghere tactică are avantajul că poate fi parţial reglementată şi că daunele vor fi limitate la un număr minim de persoane. Când interceptarea tactică este folosită pentru aplicarea legii (nu pentru spionaj), ea este folosită cel mai des pentru colectarea de probe. Probele ajung la tribunal, deci devin publice. Deci poţi, cel puţin câteodată, să monitorizezi puţin ce se întâmplă. Şi poţi interoga oamenii la tribunal

despre cum a fost colectată acea informaţie şi de ce ar trebui să presupunem că este validă. Poţi s-o ţii sub observaţie. Dar reglementarea interceptării strategice este complet absurdă. Ea este, prin definiţie, interceptarea tuturor, deci ce fel de legislaţie putem elabora dacă premisa de la care se porneşte este interceptarea tuturor?

JÉRÉMIE: Dezbaterea aceasta despre dezvăluirea completă a dosarelor mă duce cu gândul la gruparea cunoscută sub numele de Lulzăec, care a publicat 70 de milioane de dosare de la Sony – toate datele utilizatorilor Sony – şi puteai vedea toate adresele, adresele de e-mail şi parolele. Cred că erau până şi detalii ale cardurilor de credit a 70 de milioane de utilizatori. Cum sunt un activist ai drepturilor fundamentale, m-am gândit: „Ceva trebuie să fie în neregulă aici dacă, pentru a-ţi argumenta poziţia sau pentru a te amuza, faci publice datele personale ale oamenilor”. Nu mă simţeam deloc în largul meu văzând adresele de e-mail ale oamenilor din acele dosare. Am crezut cumva că acele persoane se distrau cu securitatea informatică şi că ceea ce demonstrau era că o companie cu puterea şi notorietatea lui Sony nu e în stare să păstreze secretele utilizatorilor săi, iar faptul că acele 70 de milioane de utilizatori şi-au căutat adresa de e-mail sau numele într-un motor de căutare şi au găsit acest dosar i-a făcut imediat să-şi dea seama: „Vai, ce-am făcut când am predat datele astea lui Sony? Ce înseamnă să dai date personale unei companii?”

JACOB: Iar apoi împuşcă mesagerul.

Şobolanii de la Operă

JULIAN: Am trecut prin toate aceste scenarii pesimiste, aşa că acum aş vrea să ne uităm la un scenariu potenţial utopic. Avem radicalizarea tinerilor pe internet, iar acum tinerii care sunt pe internet ajung să reprezinte

aproape majoritatea tinerilor. Pe de altă parte, avem nişte încercări disperate de anonimizare şi liberalizare a publicării, de eliminare a cenzurii – există o gamă largă de interacţiuni între stat şi sectorul privat, care luptă împotriva acestui lucru –, dar, hai să presupunem că vom urma traiectoria pozitivă. Cum va arăta situaţia în acest caz?

JACOB: Cred că avem nevoie, fără excepţie, de dreptul de a citi şi de a vorbi liber, fără să existe excepţie nici măcar în cazul unui singur om, fără nicio excepţie, pentru a-l cita greşit pe Bill Hicks.121 El a vorbit despre lucrul ăsta referitor la educaţie, îmbrăcăminte şi mâncare, dar de fapt la asta se rezumă totul: fiecare are dreptul. să citească, fiecare are dreptul să vorbească liber. Aici sunt cuprinse şi dreptul la exprimarea anonimă a opiniei, capacitatea de a face tranzacţii cu diferite persoane fără să existe intervenţii ale unor terţi, capacitatea de a călători liber, capacitatea de a corecta datele tale din diferite sisteme. Să avem transparenţă şi răspundere pentru fiecare sistem în care vedem că există orice fel de influenţă.

ANDY: Aş adăuga ideea că, odată cu creşterea numărului sistemelor de procesare a informaţiei şi a laturii lor reprezentate de reţea, şi odată cu disponibilitatea unor unelte ca Tor şi criptarea şi aşa mai departe, cantitatea datelor care poate fi suprimată este destul de mică, ceea ce înseamnă că asta e tot ce trebuie să facă guvernele, iar ele o ştiu bine. Ştiu bine că a opera în secret în zilele noastre înseamnă doar a opera în secret pentru o anumită perioadă, mai devreme sau mai târziu totul devenind public, iar acesta este un lucru bun. Aspectul acesta schimbă modul în care operează. Lucrul acesta înseamnă că ştiu că există o răspundere. De asemenea, înseamnă că

introduc în mod forţat posibilitatea denunţării în interiorul unor întreprinderi, ca în cazul legii Sarbanes-Oxiey, care cerea companiilor înregistrate la bursele din SUA să aibă o infrastructură care să permită tragerea semnalelor de alarmă, astfel încât persoanele care trebuie să semnaleze superiorilor lor comportamente infracţionale sau de altă natură să aibă o modalitate de a o face fără să fie afectate în mod direct de cei pe care îi denunţă.122 Deci e un lucru bun şi va crea, pe termen lung, mai multe procese sustenabile.

JÉRÉMIE: Continuând ideea lui Jake, cred că trebuie să clarificăm pentru toată lumea faptul că un internet liber, deschis şi universal este probabil cel mai important instrument pe care îl avem pentru a aborda problemele globale care sunt în joc, că a-l proteja este probabil una dintre sarcinile fundamentale care revin generaţiei noastre şi că atunci când cineva, undeva – fie că e guvernul sau o companie – restricţionează capacitatea unor persoane de a accesa acest internet universal, tot internetul are de suferit. Omenirea întreagă este restricţionată. Suntem martorii faptului că putem creşte împreună costurile politice ale unei astfel de decizii, iar fiecare dintre cetăţenii care accesează internetul liber poate împiedica un asemenea comportament. Începem să observăm că în calitate de cetăţeni ai reţelei avem putere în ceea ce priveşte deciziile politice şi că putem face ca guvernele noastre şi cei care sunt aleşi să ne reprezinte să fie mai responsabili de ceea ce fac atunci când iau decizii proaste care ne afectează libertăţile fundamentale şi care afectează un internet liber, global şi universal.

Aşadar, cred că ar trebui să punem aceste lucruri în practică. Ar trebui să continuăm să propagăm cunoştinţele despre cum să o facem. Ar trebui să continuăm să ne

îmbunătăţim modurile de acţiune, felul în care facem schimb de tactici în ceea ce priveşte intervenţiile în parlament, demascarea politicienilor, demascarea influenţei pe care o au lobby-urile industriale asupra procesului de elaborare de politici. Ar trebui să continuăm să construim instrumente care să le permită cetăţenilor să-şi construiască propriile infrastructuri descentralizate şi criptate, să le permită să deţină propria infrastructură de comunicaţii. Ar trebui să promovăm aceste idei în întreaga societate ca o modalitate de a clădi o lume mai bună şi deja începem să o facem – trebuie doar să continuăm.

JULIAN: Jake, dacă te uiţi la descrierea problemelor internetului făcută de persoane ca Evgeny Morozov, aceste probleme au fost prevăzute acum mult timp de către membrii mişcării cypherpunk.123 Ei nu erau de părere că trebuie doar să ne plângem de statul poliţienesc care începea să înmugurească, ci că putem, că trebuie chiar, să construim uneltele unei noi democraţii. Le putem construi de fapt cu mintea, le putem distribui altor oameni şi putem să ne construim, împreună, apărarea. Tehnologia şi ştiinţa nu sunt neutre. Există anumite forme de tehnologie care ne oferă aceste drepturi şi libertăţi fundamentale la care au sperat atât de mulţi, de atât de multă vreme.

JACOB: Desigur. Cred că lucrul fundamental cu care ar trebui să rămânem – mai cu seamă în cazul cuiva de şaisprezece sau optsprezece ani care şi-ar dori să facă din lume un loc mai bun – este că niciunul dintre cei care suntem aici şi nimeni în lumea aceasta nu s-a născut cu realizările care le vor fi mai târziu inscripţionate pe mormânt. Cu toţii construim alternative. Toţi cei care suntem aici de faţă am construit alternative şi fiecare, mai ales mulţumită internetului, are puterea să facă acest lucru în privinţa contextului în care trăieşte. Şi nu că ar

avea o datorie de a o face, dar dacă e să-şi dorească acest lucru, o poate face. Şi dacă o face, va avea un impact asupra multor oameni, mai ales în ceea ce priveşte internetul. Construirea acelor alternative implică o amplificare, o augmentare.

JULIAN: Aşadar, dacă construieşti un lucru, îl poţi oferi unui miliard de oameni pentru a-l folosi.

JACOB: Sau dacă participi la construirea unei reţele a anonimităţii – cum e reţeaua Tor, bunăoară – ajuţi la construirea alternativei comunicaţiei anonime unde înainte ea nu exista.

JÉRÉMIE: Este distribuirea liberă a cunoaşterii şi prilejuirea unor canale de comunicaţie prin care cunoaşterea să treacă liber, asta este ceea ce faci. Tor este un software liber, care este astăzi atât de răspândit pentru că înglobăm acea noţiune de libertate în modul în care construim alternative, în care construim tehnologii, în care construim modele.

JACOB: Avem nevoie de software liber pentru o lume liberă, şi avem nevoie de hardware liber şi cu sursă deschisă.

JULIAN: Dar prin liber înţelegi neîngrădit, oamenii se pot juca cu elementele interne, pot vedea cum funcţionează?

JACOB: Întocmai. Avem nevoie de software care este la fel de liber ca legile unei democraţii, astfel încât fiecare să-l poată studia, schimba, să-l poată înţelege în întregime şi să se asigure că acel software face ceea ce-şi doreşte utilizatorul să facă. Software Liber, Hardware Liber şi cu Sursă Deschisă.124

JULIAN: Cei din mişcarea cypherpunk au avut această idee că „codul este lege”.

JÉRÉMIE: Ideea e a lui Larry Lessig.

JULIAN: Pe internet, ceea ce poţi face este definit de tipul programelor care există, de tipul programelor care rulează, deci codul este lege.

JACOB: Foarte adevărat, iar acest lucru înseamnă că poţi construi alternative, mai cu seamă în ceea ce priveşte scrierea de programe, dar chiar şi în ceea ce priveşte imprimarea 3D sau chestii sociale precum locaţiile hackerspace care există.125 Poţi ajuta la construirea alternativelor, iar ceea ce este cel mai important este ca ele să intre într-un proces de normalizare, unul în care oamenii să se obişnuiască, din punct de vedere social, cu construirea propriilor obiecte 3D, cu modificarea software-ului propriu, şi unul în care sunt conştienţi că dacă cineva îi împiedică să facă acest lucru, atunci acel cineva nu furnizează acces la internet, ci furnizează un internet filtrat, cenzurat şi, de fapt, îşi încalcă obligaţia de a purta de grijă.

Asta e ceea ce fiecare dintre noi a făcut cu viaţa sa, iar oamenii ar trebui să ştie că au posibilitatea să o facă pentru generaţiile viitoare, şi pentru generaţia de acum. De asta mă aflu aici – pentru că dacă nu-l susţin acum pe Julian, în toate lucrurile prin care trece, ce fel de lume aş mai construi? Ce fel de mesaj transmit lumii când permit unor porci să mă intimideze? în niciun caz, niciodată. Trebuie să construim şi să schimbăm situaţia asta. După cum a spus Ghandi: „Fii tu însuţi schimbarea pe care vrei să o vezi în lume*, dar trebuie să fii şi tulburarea pe care vrei să o vezi în lume.126 E un citat din *A Soţier World*, nu e acelaşi cu citatul lui Ghandi, dar cred că oamenii trebuie să ştie că nu pot să stea pur şi simplu deoparte, neimplicaţi, ci trebuie să ia atitudine, şi sper că o vor face.127

ANDY: Cred că există o bună şansă ca oamenii să

continue lucrurile din punctul în care le-am adus noi, iar alternativele vin din partea oamenilor care nu sunt mulţumiţi de situaţia pe care o găsesc sau de opţiunile pe care le au.

JULIAN: Poţi vorbi puţin şi despre Chaos Computer Club în acest contenxt?

ANDY: Mereu CCC ăsta.128

JULIAN: Păi e unic în lume.

ANDY: CCC este o organizaţie galactică de hackeri care promovează libertatea accesului la informaţie, transparenţa tehnologiei şi care se preocupă de relaţia dintre dezvoltarea umană şi cea tehnologică, aşadar de interacţiunea dintre societate şi tehnologie.

JULIAN: A devenit, de fapt, politică.

ANDY: CCC a devenit un soi de forum al hackingului, cu câteva mii de membri aflaţi oarecum în Germaniadar noi nu considerăm că locuim în Germania, noi considerăm că locuim pe internet, ceea ce reprezintă, poate, o parte importantă a imaginii noastre de sine, care exercită farmecul ei. Suntem foarte bine conectaţi la alte grupuri de hackeri din Franţa, America şi din alte ţări.

JULIAN: Şi de ce crezi că a apărut în Germania? Nucleul este în Germania – de-aici s-a extins în restul lumii.

ANDY: Nemţii încearcă tot timpul să structureze totul.

JÉRÉMIE: Ingineria nemţească e mai bună.

JULIAN: Dar cred că nu este doar asta. E vorba despre Berlin, şi despre căderea blocului estic.

ANDY: Are de-a face cu mai multe lucruri. Germania a făcut cel mai rău lucru pe care îl poate face o ţară altor oameni, deci e poate puţin mai imună la repetarea acelor lucruri – lucruri precum intrarea în război cu alte ţări. Am

făcut toate aceste lucruri, am trecut prin asta, am fost pedepsiţi aspru şi a trebuit să învăţăm de pe urma acestei experienţe, iar felul acesta descentralizat de a gândi şi comportamentul antifascist, cum ar fi prevenirea unui stat totalitar, încă sunt predate în şcolile Germaniei din cauză că am avut experienţa acelor lucruri la cel mai rău nivel. Deci cred că, în parte, aşa ar trebui să înţelegem CCC-ul, care este oarecum un fenomen german. Wau Holland, cel care a fondat CCC, a avut şi o abordare foarte pronunţat politică în privinţa sa. L-am întâlnit la mormântul lui Wau pe tatăl său, deoarece fiul a murit înaintea sa, iar tatăl său nu a avut de spus cuvinte plăcute. A spus: „... şi ca niciodată să nu mai existe activităţi totalitare, antipacifiste pe teritoriul german”. Acesta a fost comentariul tatălui când şi-a îngropat fiul, iar acest lucru mi-a lămurit multe despre motivul pentru care Wau a fost atât de hotărât să influenţeze oamenii şi să aibă grijă de ei, să se comporte în mod paşnic cu ceilalţi, răspândind idei, nu limitându-le, fără să fie agresiv, ci cooperant.

Iar ideea creării în mod cooperant a unor lucruri – cum ar fi mişcările pentru sursă deschisă – a infectat într-adevăr ideile mişcării cypherpunk americane şi s-a unit cu ele şi cu cele ale lui Julian Assange/Wikileaks şi aşa mai departe. Ceea ce se întâmplă acum este ceva global, şi există atitudini culturale foarte diferite, foarte descentralizate, ale unor hackeri elveţieni, germani, italieni – iar acesta este un lucru bun. Hackerii italieni se comportă complet diferit faţă de hackerii germani – oriunde ar fi, trebuie să gătească bine; hackerii germani trebuie să aibă totul bine structurat. Nu spun că unii sunt mai buni decât ceilalţi, vreau doar să spun că fiecare dintre aceste culturi descentralizate are părţile ei foarte frumoase. La conferinţa hackerilor italieni poţi merge în

bucătărie şi vei vedea acolo un loc minunat; la tabăra germană de hacking vei găsi un internet minunat, dar ai face bine să nu te uiţi în bucătărie. Oricum, esenţa lucrurilor este că noi creăm. Şi cred că ne aflăm într-un soi de conştiinţă comună care este cât se poate de îndepărtată faţă de identitatea noastră naţională – aceea de nemţi sau italieni sau americani sau mai ştiu eu ce –, vedem doar că ne dorim să rezolvăm problemele, ne dorim să lucrăm împreună. Vedem această cenzură a internetului, această luptă a guvernelor împotriva tehnologiilor noi, ca pe un soi de situaţie evolutivă pe care trebuie să o depăşim.

Şi suntem pe cale să identificăm şi soluţii, nu doar probleme, ceea ce e bine. Probabil că încă va trebui, în următorii cine ştie câţi ani, să luptăm împotriva multor tâmpenii, dar acum, în sfârşit, a apărut o generaţie de politicieni care nu văd internetul ca pe un duşman, ci înţeleg că el face parte din soluţie, nu din problemă. Lumea noastră încă este construită pe armament, pe puterea secretelor, pe un întreg cadru economic şi aşa mai departe, dar lucrul acesta se schimbă şi chiar cred că jucăm un rol foarte important în procesul actual de elaborare de politici. Putem discuta despre aceste probleme într-o manieră controversată – iar acesta este un lucru pe care CCC-ul a reuşit să-l facă de multă vreme încoace. Nu suntem un grup omogen, avem opinii foarte diferite. Îmi place că stăm aici împreună şi că nu formulăm cele mai bune răspunsuri imediat, formulăm mai degrabă întrebări şi ne punem fiecare ideile la bătaie şi vedem care e concluzia. Acesta este genul de proces care trebuie să continue, iar pentru aceasta avem nevoie de un internet liber.

JULIAN: M-am întrebat care ar fi traiectoria pozitivă pentru viitor. Autocunoaştere, diversitate şi reţele de

autodeterminare. O populaţie globală educată – nu vreau să spun educată în mod formal, ci educată în sensul înţelegerii felului în care funcţionează civilizaţia omenească la nivel politic, industrial, ştiinţific şi psihologic – ca rezultat al schimbului liber de comunicaţii, stimulând de asemenea culturi noi şi pline de viaţă şi diversificarea maximă a gândirii individuale, autodeterminare regională sporită şi autodeterminare a grupurilor de interese care pot să interacţioneze repede şi pot face schimb de valori rapid, peste hotarele geografice. Şi poate că lucrurile acestea şi-au găsit expresia în Primăvara Arabă şi în activismul panarab care a fost amplificat de internet, în cadrul colaborării noastre cu Nawaat.org, cei care au creat Tunileaks, eliberând de sub cenzura regimului telegramele departamentului de stat din Tunisia prerevoluţionară, am văzut din proprie experienţă puterea pe care o are reţeaua de a trimite informaţia acolo unde este necesară, şi a fost o recompensă uriaşă faptul de a mă fi aflat, mulţumită eforturilor noastre, în poziţia de a putea contribui la ceea ce începea să se întâmple acolo.129 Nu văd acea luptă pentru autodeterminare ca fiind diferită de a noastră.

Această traiectorie pozitivă ar impune cunoaşterea de sine a civilizaţiei umane, deoarece trecutul nu poate fi distrus. Ar însemna imposibilitatea apariţiei statelor neo-totalitare, datorită mişcării libere a informaţiei, capacitatea oamenilor de a vorbi în privat unii cu alţii şi de a conspira împotriva unor astfel de tendinţe şi capacitatea microcapitalului de a se scurge fără a fi controlat din astfel de locuri ostile oamenilor.

Pe aceste fundaţii poate fi construită o gamă largă de sisteme politice. Pentru mine utopia ar fi o distopie dacă ar fi doar una. Sunt de părere că idealurile utopice trebuie să însemne o diversitate de sisteme şi de modele de

interacţiune. Dacă ar fi să ne uităm la dezvoltarea efervescentă a unor noi produse culturale şi chiar la schimbarea lingvistică, la subculturi care-şi elaborează propriile mecanisme de interacţiune alimentate de internet, atunci pot spune că da, această cale pozitivă pare să se deschidă.

Dar cred că, cel mai probabil, tendinţele spre omogenizare, universalitate, spre transformarea întregii civilizaţii omeneşti într-o singură piaţă vor aduce, pentru fiecare serviciu sau produs, factori normali de piaţă, cum ar fi un lider de piaţă, un al doilea, un al treilea jucător – care va fi unul de nişă, iar apoi nişte codaşi care nu au niciun cuvânt de spus. Cred că aceasta ar putea să aducă o masivă omogenizare lingvistică, o masivă omogenizare culturală, o standardizare masivă pentru a face ca aceste schimbări rapide să fie eficiente. Deci cred că scenariul pesimist este de asemenea probabil, iar statul poliţienesc transnaţional şi nesfârşitele războaie cu dronă se apropie şi ele.

De fapt, îmi amintesc de o seară în care m-am furişat la teatrul de operă din Sydney pentru a vedea piesa *Faust*. Opera din Sydney este foarte frumoasă pe timp de noapte, cu interiorul său măreţ şi luminile strălucind peste apă, spre cerul înstelat. După spectacol, am ieşit afară şi am auzit trei doamne care discutau, aplecate pe balustrada care domina golful întunecat. Doamna mai în vârstă vorbea despre problemele pe care le avea la locul de muncă, loc care s-a dovedit a fi la CIA, un post de agent secret, şi despre faptul că se plânsese la Comisia de Informaţii a Senatului SUA şi aşa mai departe, şi spunea toate aceste lucruri, în şoaptă, nepoatei sale şi unei alte doamne. Şi m-am gândit: „Deci e adevărat. Agenţii CIA chiar îşi petrec timpul la teatrul de operă din Sydney!” Şi apoi m-am uitat

în interiorul operei prin uriaşele panouri de sticlă ale faţadei, iar acolo, în tot acel rafinament somptuos şi solitar, era un şobolan de apă care se furişase în interiorul operei şi care alerga încoace şi-ncolo, sărind pe mesele acoperite cu pânză fină şi ciugulind din mâncarea Operei, sărind pe ghişeul unde erau toate biletele şi simţindu-se de minune. Şi cred că acesta este cel mai probabil scenariu pentru viitor: o structură extrem de restrictivă, omogenizată, postmodernă, transnaţională şi totalitară de o complexitate de necrezut, absurdă şi devalorizată, iar în interiorul acestei complexităţi incredibile, un spaţiu în care pot ajunge doar şobolanii isteţi.

Acesta este un aspect pozitiv al unei traiectorii negative, traiectoria negativă fiind un stat poliţienesc transnaţional, ticsit cu drone, un neofeudalism în reţea al elitei transnaţionale – nu în sensul clasic al cuvântului, ci în sensul unei interacţiuni complexe, multipartite, care a apărut ca urmare a delimitării mai multor elite naţionale faţă de populaţia comună şi a unirii între ele a acestor elite. Toate comunicaţiile vor fi supravegheate, stocate pe veci, urmărite în permanenţă, fiecare individ, în toate interacţiunile sale, va fi identificat ca acel individ, de la naştere până la moarte, de către aceste noi cercuri conducătoare. Aceasta este o schimbare majoră, chiar în raport cu ceea ce era acum zece ani, şi practic suntem deja acolo. Cred că acest lucru nu poate produce decât o atmosferă de control strict. Dacă toate informaţiile care au fost adunate despre lumea în care trăim ar fi publice, acest lucru ar putea reechilibra dinamica puterii şi ne-ar permite, în calitate de civilizaţie globală, să ne modelăm propriul destin. Dar fără o schimbare dramatică acest lucru nu se va întâmpla. Supravegherea în masă se aplică, în proporţii diferite, celor mai mulţi dintre noi, transferând

putere către cei din interiorul sistemului care însă, cred eu, nu se vor bucura nici ei prea mult de această minunată lume nouă. Acest sistem va coincide şi cu o cursă a înarmării cu drone care va elimina hotarele clar definite aşa cum le ştim astăzi, fiindcă aceste hotare sunt rezultatul contestării unor delimitări fizice, iar rezultatul va fi un război perpetuu în care reţelele de influenţă victorioase vor începe să stoarcă concesii de la lume.

Iar pe lângă aceasta, oamenii vor fi pur şi simplu îngropaţi sub imposibila matematică a birocraţiei.

Cum poate o persoană normală să fie liberă într-un astfel de sistem? Pur şi simplu nu poate, este imposibil. Nu că am putea fi complet liberi vreodată, în orice sistem, dar libertăţile pentru care am evoluat din punct de vedere biologic şi libertăţile cu care ne-am obişnuit din punct de vedere cultural vor fi eliminate aproape în întregime. Deci cred că singurii oameni care vor reuşi să-şi păstreze libertatea pe care am avut-o, să spunem, acum douăzeci de ani – pentru că sistemul de supraveghere a eliminat deja o mare parte a ei, noi pur şi simplu nu ne dăm seama încă – vor fi cei care vor fi educaţi în ceea ce priveşte funcţionarea internă a sistemului. Prin urmare, doar o elită de rebeli high-tech va rămâne liberă, aceşti şobolani isteţi care fug prin clădirea Operei.

Note

1. Simplu spus, criptografia, provenind de la termenul grecesc care înseamnă „scriere secretă”, este practica comunicării codate.

2. „Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-fi Now in the OED”, Resource Shelf, 16 septembrie 2006: http://web. resourceshelf.com/go/resourceblog/ 43743 (accesat în data de 24 octombrie 2012)

3. Wikileaks: http://wikileaks.org

4. Pentru mai multe informaţii despre fişierul *Rubberhose*, vezi: „The Idiot Savants Guide to Rubberhose”, Suelette Dreyfus: http://marutukku.org/current/src/doc/maruguide/îl.html (accesat în 14 octombrie 2012)

5. Pentru mai multe informaţii despre cartea *Underground*, vezi http://www.underground-book.net

Pentru mai multe informaţii despre filmul *Underground*: *The Julian Assange Story*, vezi: „The Internet Movie Database”: http://www.undb.com/tide/tt2357453/ (accesat în data de 21 octombrie 2012)

6. Noisebridge este un spaţiu virtual pentru hacking, cu baza în San Francisco, şi furnizor de infrastructură pentru proiecte tehnico-creative, condus colaborativ de membrii săi: https://www.noisebridge.net/wiki/Noisebridge

Chaos Computer Club din Berlin este ramura din Berlin a Chaos Computer Club (mai multe informaţii la adresa): https://Berlin. cec.de/wiki/ Chaos Computer Club Berlin.

7. Proiectul Tor: https://www.torproject.org

8. Chaos Computer Club este cea mai mare asociaţie de hacking din Europa. Activităţile sale variază de la cercetare şi explorare de natură tehnică până la campanii, evenimente, publicaţii şi consultanţă politică: http://www.cec.de.

9. EDRI: http://www.edri.org

10. ICANN: http://www.icann.org

11. buggedplanet: http://buggedplanet.info

12. Cryptophone: http://www.cryptophone.de

13. La Quadrature du Net: http://www.laquadrature.net

14. Collateral Murder: http://www.collateralmurder.com The Iraq War Logs: http://wikileaks.org/irq

The Afghan War Diary: http://wikileaks.org/afg Cablegate: http://wikileaks.org/cablegate.html

15. „Congressional committee holds hearing on national security leak prevention and punishment", Reporters Committee for Freedom of the Press, 11 iulie 2012: http://www.refp.org/browse-media-law-resources/news/ congressional-committee-holds-hearing-national-security-leak-prevent (accesat în data de 21 octombrie 2012).

16. Pentru mai multe informaţii despre Marele Juriu pentru Wikileaks, vezi lista cronologică a jurnalistei freelance Alexa O'Brien la: http://www.alexaobrien.com/timeline us versus manning assange wiki-leaks 2012.html (accesat în data de 22 octombrie 2012).

17. „*Bradley Mannings treatment was cruel and înhuman, UN torture chief rules*", *Guardian*, 12 martie 2012: http://www.guardian.co.uk/world/ 2012/mar/12/bradley-manning-cruel-inhuman-treatment-un (accesat în data de 24 octombrie, 2012).

18. „Wikileaks: guilty parties «should face death penalty»", *Telegraph*, 1 decembrie 2010: http://www.telegraph.co.uk/news/worldnews/wiki Leaks/8172916/Wikileaks-guilty-parties-should-face-death-penalty.html (accesat în data de 22 octombrie, 2012).

19. „CIA launches task force to assess impact of U.S. cables exposure by Wikileaks", *Washington Post*, 22 decembrie 2012: http://www.Washingtonpost.com/wp – dyn/content/article/2010/12/21 / AR2010122104599.

html? hpid = topnews & sid = ST2010122105304

(accesat în data de 22 octombrie 2012).

20. „Wikileaks fights to stay online after US company withdraws domain name", *Guardian*, 3 decembrie 2012: http://www.guardian.co.uk/media/ blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns (accesat în data de 23 octombrie 2012).

21. „Don't Look, Don't Read: Government Warns Its Workers Away From Wikileaks Documents", *New York Times*, 4 decembrie 2010: http://www.nytimes.com/2010/12/05/world/05 restrict.html? hp & r = 2 & (accesat în data de 23 octombrie 2012).

22. „Banking Blockade", Wikileaks: http://www.wikileaks.org/Banking-Blockade.html (accesat în data de 22 octombrie 2012).

23. Relatarea scrisă a reţinerilor lui Jacob este o lectură recomandabilă. Vezi: *„Air Space – a trip through an airport de*tention *center*", boingboing, 31 octombrie 2011: http://boingboing.net/2011/10/31/air-space-a-tripthrough-an-ai.html

De asemenea, este important în acest sens şi un interviu cu Jacob despre reţinerile sale, acordat publicaţiei *Democracy Now*: „National Security Agency Whisdeblower William Binney on Growing State Surveillance", *Democracy Now*, 20 aprilie 2012: http://www.democracynow. Org/2012/4/20/ exclusive national security agency whistleblower William (ambele linkuri au fost accesate în data de 13 octombrie 2012).

24. În mod oficial, cazul este cunoscut ca In the Matter of the 2703 (d) Order Relating to Twitter Accounts [Chestiunea Ordinului 2703 (d), referitor la conturile Twitter]: Wikileaks Rop G IOERROR; şi BirgittaJ.

25. „Secret orders target e-mail", *Wall Street Journal*,

9 octombrie 2011: http://online. wsi.com/article/ZB 10001424052970203476804576613284007315072.html (accesat în data de 22 octombrie 2012).

26. „Twitter Ordered to Yield Data în Wikileaks Case", *New York Times*, 10 noiembrie, 2011: https://www.nytimes.com/2011/11/11/ technology/ twitter-ordered-to-yield-data-in-wikileaks-case.html? r = l (accesat în data de 22 octombrie 2012).

27. „ACLU and EFF to Appeal Secrecy Ruling în Twitter/Wikileaks Case", *Electronic Frontier Foundation*, 20 ianuarie 2012: http's: //www.est.org/ press/releases/adu-eff-appeal-secrecy-ruling-twitter-wikileaks-case (accesat în data de 22 octombrie 2012)

28. Este vorba despre protestul din 6 aprilie 2008, organizat pentru a susţine greva înăbuşită a muncitorilor de la fabrica de textile Mahalla al-Kobra. Cu puţin timp înaintea protestului, „Mişcarea Tinerilor 6 Aprilie" s-a format ca grup pe Facebook, conceput pentru a încuraja oamenii să protesteze în Cairo şi în alte oraşe pentru a coincide cu acţiunea industrială din Mahalla. Protestele nu au mers conform planului, iar administratorii grupului de Facebook, Esraa Abdel Fattah, Ahmed Rashid şi Ahmed Maher au fost arestaţi, împreună cu alţii. Maher a fost torturat pentru parola contului său de Facebook. Mişcarea Tinerilor 6 Aprilie a jucat un rol şi în revoluţia egipteană din 2011. Vezi: „Cairo Activists Use Facebook to Rattle Regime", *Wired*, 20 octombrie 2008: http://www.wired.com/techbiz/startups/ magazine/16-ll/fi facebook-egypt? current-Page = all (accesat în data de 23 octombrie 2012).

29. „*Cum să protestezi inteligent**, autori anonimi, distribuit la începutul revoltei de optsprezece zile care l-a înlăturat de la putere pe preşedintele Mubarak (varianta în

arabă): http://www.itstime.it/Approfondimenti/Egyptian-Revolution Manualpdf. Fragmente din acest document au fost traduse şi în engleză. şi publicate la: „Egyptian Activists Action Plan: Translated”, *Atlantic*, 27 ianuarie 2011: http://www.theadantic.com/international/archive/2011/01 / egyptian-activists-acţion-plan-translated/70388 (ambele linkuri au fost accesate în data de 23 octombrie 2012).

30. Panopticonul este o închisoare inventată de filosoful Jeremy Bentham în 1787, proiectată în aşa fel încât să permită unui singur gardian să supravegheze toţi prizonierii în acelaşi timp, pe ascuns, privindu-i. Jeremy Bentham (editat de Miran Bozovic), *The Panopticon Writings* (Verso, 1995), disponibil online la: http://cartome.org/panopticon2.htm (accesat în data de 22 octombrie 2012).

31. Johannes Gutenberg (1398 – 1468) a fost un fierar german care a inventat tiparul cu caractere mobile, o invenţie care a dus la unele dintre cele mai semnificative schimbări sociale din istorie. Invenţia presei de tipar este corespondentul istoric cel mai apropiat al invenţiei internetului.

32. John Gilmore este unul dintre primii cypherpunks, unul dintre fondatorii Electronic Frontier Foundation şi activist pentru libertăţile civile. Fraza citată de Andy a fost citată prima dată în „First Nation in Cyberspace”, *Time Magazine*, 6 decembrie 1993. Vezi site-ul lui John Gilmore: http://www.toad.com/gnu (accesat în data de 22 octombrie 2012).

33. „Tehnologia proprietară este orice fel de sistem, instrument sau proces tehnic care este dezvoltat deşi pentru o afacere anume […] Ideile dezvoltate şi predate de către angajaţi sunt considerate de obicei proprietatea

intelectuală a angajatorului, lucru care le permite să se numească tehnologii proprietare". Definiţie preluată de la wise GEEK: http://www.wisegeek.com/what-is-proprietary-technology.htm (accesat în data de 22 octombrie 2012).

34. Cory Doctorow, „The coming war on general-purpose computing", boingboing, 10 ianuarie 2012 (bazat pe un discurs important ţinut la Chaos Computer Congress, în decembrie 2011): http://boing-boing.net/2012/01 /10/lockdown.html (accesat în data de 15 octombrie 2012).

35. Stuxnet este un virus de calculator foarte sofisticat, despre care se crede că a fost elaborat de SUA şi Israel pentru a ataca echipamentul Siemens despre care se presupunea că ar fi folosit de Iran pentru îmbogăţirea uraniului. Pentru o expunere de ansamblu, vezi Wikipedia: http://en.wikipedia.org/ wiki/Stuxnet. Vezi, de asemenea, „Wikileaks: US advised to sabotage Iran nuclear sites by German thinktank", *Guardian*, 18 ianuarie 2011: http://www.guardian.co.uk/world/2011 /jan/18/wikileaks-us-embassy-cable-iran-nudear.

Wikileaks a publicat unul dintre primele rapoarte despre efectele despre care se crede acum că sunt un rezultat al Stuxnet – accidentul de la centrala nucleară de la Natanz, în Iran. Vezi „Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation", Wikileaks, 17 iulie 2009: http://wikileaks.org/wiki/Serious nuclear accident may lay behind Iranian nuke chief%27 s mystery resignation.

Dovezile provenind de la compania de spionaj global Stratfor, scurse de Wikileaks, indică implicarea israeliană. Vezi „E-mail ID 185945, The Global Intelligence Files": http://wikileaks.org/gifiles/docs/185945 realpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html (toate

linkurile au fost accesate în data de 16 octombrie 2012).

36. „Pentesting”, prescurtarea de la „penetration testing” [teste de penetrare] este un termen din ingineria de securitate care desemnează organizarea legală, autorizată a unui atac împotriva unui sistem informatic sau împotriva unei reţele de computere, aşa cum ar face-o un utilizator neautorizat, pentru a evalua cât este aceasta de sigură. Cercetătorii în materie de securitate sunt recrutaţi deseori din comunitatea de hackeri pentru a face teste de penetrare pe sisteme sigure.

37. Prinde Steagul este la origine un joc jucat afară, în aer liber, în care de obicei două echipe trebuie să apere o bază şi să păzească un steag. Obiectivul este să prindă steagul celeilalte echipe şi să se întoarcă cu el la bază. La conferinţele de hackeri se joacă o versiune computerizată, unde echipele atacă şi apără sisteme şi reţele informatice.

38. Cupa Sysadmin este o prescurtare de la System Administrator Cup. Un administrator de sistem este o persoană care lucrează în domeniul IT şi întreţine sau operează un sistem sau o reţea informatică. Jacob vrea să spună că exerciţiul era ca un turneu pentru administratori de sistem.

39. „Aaron spune că criptarea protejează confidenţialitatea, comerţul”, USIS Washington File, 13 octombrie 1998: http://www.fas.org/irp/news/1998/10/98101306 cât.html (accesat în data de 21 octombrie 2012).

40. Site-ul Acordului de la Wassenaar: http://www.wassenaar.org (accesat în data de 21 octombrie 2012).

41. Andy se referă la diverse evenimente ale „Primului Război Criptografic” al anilor ’90. Când activiştii cypherpunk au început să răspândească instrumente

puternice de criptografiere cum ar fi software-ul liber, administraţia SUA a luat măsuri pentru a împiedica utilizarea cu succes a instrumentelor criptografice. A numit criptografia muniţie şi i-a restricţionat exportul; a încercat să introducă tehnologii concurente care erau stricate în mod intenţionat, în aşa fel încât reprezentanţii legii să poată descifra informaţiile; şi a încercat să introducă controversata schemă „key escrow”. O scurtă vreme după trecerea în noul secol s-a crezut în general că acele eforturi au fost învinse definitiv. Cu toate acestea, acum are loc un „Al Doilea Război Criptografic”, împreună cu eforturi legislative şi tehnice de a sabota sau marginaliza folosirea criptografiei.

42. Exemplul de calcul a fost făcut pentru cele 196, 4 miliarde de minute de apeluri de pe fix efectuate în Germania în 2010, digitalizate cu un codec audio de 8 Kbps, care însumau o cantitate de 11 784 Petabiţi (Pb), rotunjiţi (cu tot cu consumul suplimentar) la 15 Pb. Presupunând costuri aproximative de stocare de 500.000 USD (500 kUSD) pentru un Pb, ajungem la suma de 7, 5 milioane USD, sau în jur de 6 milioane EUR. La aceasta se mai adaugă costurile unui echipament informatic decent al centrului de date, costurile puterii de procesare, conexiunilor şi ale angajaţilor. Chiar dacă se includ şi cele 101 miliarde de minute de apeluri mobile din Germania, cu încă 50 Pb şi 18, 3 milioane EUR, preţul rămâne mai mic decât cel al unui avion militar ca Eurofighter (90 de milioane EUR) sau F22 (150 de milioane USD).

43. Pentru mai multe informaţii despre VAST – ech vezi site-ul buggedplanet: http://buggedplanet.info/index.php? title = VASTECH (accesat în data de 21 octombrie 2012).

44. Scandalul supravegherii domestice fără mandat

de către NSA este cel mai important caz de supraveghere în masă din istoria Statelor Unite. Legea Foreign Intelligence Surveillance Act din 1978 (FISA) a declarat ca fiind ilegale acţiunile de spionaj fără mandat ale agenţiilor SUA împotriva cetăţenilor SUA. După atentatele din 11 septembrie, Agenţia Naţională de Securitate a început să încalce masiv prevederile FISA, autorizată printr-un ordin executiv secret al lui George W. Bush. Administraţia Bush şi-a revendicat autoritatea executivă de a face aceste lucruri sub prevederile legislaţiei de urgenţă votate în 2001 de Congres: The Authorization for the Use of Military Force (AUMF) [Autorizaţia pentru Folosirea Forţei Militare] şi PATRIOT ACT. Programul de spionaj fără mandat al NSA – care implica cooperarea din partea unor firme private, cum ar fi AT & T – a rămas secret până în 2005, când a fost denunţat de New York Times. Vezi» *Bush Lets U.S. Spy on Callers Without Courts*" *New York Timesy* 16 decembrie 2005: http://www.nytimes.com/2005/12/16/politics/16 program.html? pagewanted = all.

Unii reporteri ai *New York Times* fuseseră contactaţi anonim de cineva care scursese informaţii despre existenţa programului de supraveghere fără mandat. În 2004, Bill Keller, director executiv al *New York Times* la vremea aceea, a acceptat, la cererea administraţiei Bush, să nu publice ştirea timp de un an, până când Bush va fi fost ales din nou. În 2005, *New York Times* s-a grăbit să publice articolul când a aflat că administraţia ar fi pe cale să elaboreze un ordin de restricţie, cum fusese cel din cazul Pentagon Papers. Administraţia Bush a negat că ar fi fost comisă vreo ilegalitate în programul NSA. Departamentul de Justiţie a lansat imediat o anchetă pentru a găsi sursa scurgerii, care a implicat douăzeci şi cinci de agenţi

federali şi cinci procurori. Unii membri din conducerea Partidului Republican au cerut urmărirea în justiţie a publicaţiei *New York Times* sub prevederile Legii Spionajului.

Ca urmare a publicării articolului în *New York Times*, alte denunţuri au apărut în presă, alcătuind treptat imaginea nelegiuirii şi a risipei la cele mai înalte niveluri ale NSA. Grupări militante ca American Civil Liberties Union (ACLU) şi Electronic Frontier Foundation (EFF) au intentat o serie de procese în instanţă. Într-unul dintre aceste procese, ACLU *versus* NSA, reclamanţilor le-a fost negată plângerea din cauză că nu puteau dovedi că fuseseră spionaţi personal. Într-un alt proces, Hepting versus AT & T, Mark Klein, un angajat al AT & T, a adus în instanţă un afidavit care dezvăluia dimensiunile cooperării dintre AT & T şi programul de spionare domestică. Vezi secţiunea destinată companiei AT & T de pe site-ul EFF: https://www.est.org/cases/hepting.

Mark Klein a fost martor în cazul Hepting *versus* AT & T. Ca fost angajat al AT & T, care lucrase în Folsom, San Francisco, declaraţia sa, făcută organizaţiei EFF în cazul Hepting *versus* AT & T, a scos la iveală existenţa „Camerei 64IA”, o instalaţie de interceptare strategică operată de AT & T pentru NSA. Instalaţia permitea accesul la conducte de fibră optică ce conţineau reţeaua principală a traficului de internet, oferind capacitatea de a supraveghea tot traficul de internet care intra şi ieşea din clădire, atât cel extern, cât şi cel intern. Alt informator împotriva NSA, William Binney, a estimat că există până la 20 de astfel de instalaţii, toate plasate în puncte strategice în reţeaua de telecomunicaţii a Statelor Unite.

Declaraţia lui Klein oferă informaţii importante despre programul de supraveghere al NSA, confirmat de

alţi informatori împotriva NSA. Acesta este un exemplu de „interceptare strategică” – tot traficul de internet care trece prin Statele Unite este copiat şi stocat pe o perioadă nelimitată. Se poate şti cu certitudine că traficul domestic al SUA este de asemenea interceptat şi stocat pentru că, din punctul de vedere al tehnologiei, când se lucrează cu un trafic de un asemenea volum, este imposibil să se trieze traficul pentru care ar fi necesar un mandat FISA. Interpretarea oficială a legii FISA afirmă acum că a avut loc o „interceptare” doar atunci când o comunicaţie domestică deja interceptată şi stocată de către NSA este „accesată” în baza de date a NSA, şi că doar în acest caz este necesar un mandat. Cetăţenii SUA ar trebui să plece de la premisa că tot traficul telecomunicaţiilor (inclusiv apelurile telefonice, mesajele SMS, e-mailurile şi navigarea pe internet) este monitorizat şi stocat pentru totdeauna în centrele de date ale NSA.

În 2008, ca reacţie la numărul mare de litigii rezultat din scandalul acesta, Congresul SUA a aprobat o serie de amendamente la legea FISA din 1978 care au fost semnate imediat de preşedinte. Acestea au creat temeiul pentru acordarea unei „imunităţi retroactive” foarte controversate împotriva urmăririi în justiţie pentru încălcarea FISA. în timpul campaniei sale prezidenţiale, senatorul Barack Obama făcuse din „transparenţă” o parte importantă a programului său şi a promis să protejeze denunţătorii, dar când a venit la putere în 2009, Departamentul de justiţie a continuat politicile administraţiei Bush, ieşind într-un final victorios în cazul Hepting, dar şi în altele, prin acordarea „imunităţii retroactive” companiei AT & T.

Deşi investigaţia Departamentului de Justiţie pentru a găsi sursa primului articol al *New York Times* a eşuat în ceea ce priveşte găsirea informatorului anonim, ea a dus la

găsirea altora, care ieşiseră la lumină după apariţia articolului. Unul dintre ei era Thomas Drake, fost angajat al NSA într-o funcţie de conducere executivă, care reclamase ani de zile Comisiei Congresionale pentru Monitorizarea Spionajului corupţia şi risipa din programul „Trailblazer" condus de NSA. Reclamaţiile interne au fost înăbuşite, după cum au fost şi toţi funcţionarii statului care doreau să continue cercetările în privinţa lor. După articolul din *New York Times*, Drake dezvăluise situaţia programului Trailblazer ziarului *Baltimore Sun*. 1 a fost pus sub acuzaţie în urma unei investigaţii a Marelui Juriu, desemnat drept „inamic al statului" şi condamnat sub prevederile Legii Spionajului. Vezi „The Secret Sharer", *New Yorker*, 23 mai 2011: http://www.newyorker.com/reporting/ 2011/05/23/110523 fa fact mă-yer? current Page = all.

Urmărirea penală a lui Drake s-a prăbuşit în urma unei intense examinări publice care a avut loc în iunie 2011, iar după diverse încercări eşuate de a-l obliga pe Drake să accepte o înţelegere cu procurorul, Departamentul de Justiţie s-a mulţumit cu pledoaria sa de vinovăţie referitoare la o abatere minoră. Drake a primit un an cu suspendare.

Efectul negativ al scandalului supravegherii NSA continuă. Organizaţia ACLU se află în litigiu pentru a contesta constituţionalitatea amendamentelor FISA din 2008 în procesul Amnesty el. *al*. *versus* Clapper. Vezi „FISA Amendment Act Challenge", ACLU, 24 septembrie 2012: http://www.aclu.org/national-security/amnesty-et-al-v-clapper.

În cazul Jewel *versus* NSA, EFF încearcă să pună capăt supravegherii fără mandat a NSA. Procesul a fost respins în 2009 după ce administraţia Obama şi-a susţinut

imunitatea în virtutea unor secrete de stat. Vezi pagina EFF despre procesul Jewel *versus* NSA: https://www.est.org/cases/jewel. Totuşi, Curtea de Apel pentru cel De-al Nouălea Circuit a permis redeschiderea cazului în decembrie 2011. Thomas Drake şi alţi informatori împotriva NSA, William Binney şi J. Kirk, depun mărturie în cazul Jewel *versus* NSA. Administraţia Obama – care şi-a făcut campanie cu un program pentru transparenţă – a urmărit penal mai mulţi denunţători sub prevederile Legii Spionajului decât toate celelalte administraţii luate împreună. (Toate linkurile din această notă au fost accesate în data de 23 octombrie 2012.)

45. Vezi pagina despre sistemul Eagle pe buggedplanet: http://buggedplanet. info/index.php? tide = AMESYSS – trate-gic.28.22 Massive.22.29 Appliances (accesat în data de 22 octombrie 2012).

46. „Istanţa judecătorească germană ordonă ştergerea datelor telecomunicaţiilor stocate", BBC, 2 martie 2010: http://news. bbe.co. Uk/l/hi/world/ Europe/8545772. stm (accesat în data de 15 octombrie 2012).

47. Directiva 2006/24/EC a Parlamentului şi Consiliului European cere statelor europene să reţină datele telecomunicaţiilor cetăţenilor lor pe o perioadă între şase şi douăzeci şi patru de luni. Aplicarea acestei directive în Germania a fost declarată neconstituţională. În mai 2012, Comisia EU a intentat un proces la Curtea Europeană de Justiţie în cazul Germaniei pentru că nu s-a conformat directivei (vezi publicaţia de presă a Comisiei: http://Europa.eu/rapid/press-release IP-12 – 530 en.htm, accesată în data de 15 octombrie 2012).

48. Vezi „Suedia aprobă legea monitorizării telecomunicaţiilor", BBC, 19 iunie 2008: http://news.

bbe.co.uk/1 /hi/world/Europe/7463333. stm. Pentru mai multe informaţii despre FRA-lagen, vezi Wikipedia: http://en.wikipedia.org/wiki/FRA law (ambele linkuri au fost accesate în data de 10 octombrie 2012).

49. Metadatele sunt „date despre date". În contextul acestei discuţii, metadatele se referă la alte date decât „conţinutul" comunicării electronice. Este aspectul exterior al plicului, nu conţinutul său. Supravegherea metadatelor nu vizează conţinutul e-mailurilor, ci mai degrabă toate informaţiile din jurul conţinutului – cui a fost trimis e-mailul sau de către cine, adresa IP (deci locaţia) de unde a fost trimis, ora şi data fiecărui e-mail etc. Ideea este însă că tehnologia pentru interceptarea metadatelor este aceeaşi cu tehnologia pentru interceptarea conţinutului. Dacă acorzi cuiva dreptul să-ţi supravegheze metadatele, echipamentul lor trebuie să intercepteze şi conţinutul comunicaţiilor tale. În afară de acest lucru, majoritatea persoanelor nu înţeleg că „metadatele luate ca întreg înseamnă conţinut" – când toate metadatele sunt puse la un loc se produce o imagine extrem de detaliată a comunicaţiilor cuiva.

50. Amesys face parte din gruparea Bull, care făcea cândva concurenţă Dehomag-ului, o filială a IBM, în ceea ce priveşte vânzarea sistemelor cu cartele perforate naziştilor. Vezi Edwin Black, *IBM and the Holocaust* (Crown Books, 2001). Pentru mai multe informaţii despre spionarea de către Gaddafi a cetăţenilor libanezi din Regatul Unit folosind echipament de supraveghere Amesys, vezi „Exclusive: How Gaddafi Spied on the Fathers of the New Libya", OWNI.eu, 1 decembrie 2011: http:// owni. eu/2011/12/01 / exclusive-how-gaddafi-spied-on-the-fathers-of-the-newlibya (accesat în data de 22 octombrie 2012).

51. Wikileaks a început să publice în decembrie 2011 „The Spy Files”, dezvăluind dimensiunile supravegherii în masă. Acestea pot fi accesate la http:// wikileaks.org/the-spyfiles.html.

52. Pentru mai multe detalii vezi buggedplanet: http://buggedplanet.info/index.php? title = LY

53. Congresul Chaos Communication este întâlnirea anuală a comunităţii internaţionale a hackerilor, organizată de Chaos Computer Club.

54. Jacob se referă la ZTE, unul din cei doi producători chinezi de bunuri electronice (celălalt fiind Huawei) care sunt suspectaţi de multă lume că ar fi vulnerabile la accesarea datelor lor de către cineva neautorizat. Jacob sugerează că infrastructura de comunicaţii primită „cadou” are un cost – faptul că va fi, prin însăşi alcătuirea sa, susceptibilă supravegherii chineze.

55. Kill Your Television este numele unei forme de protest împotriva comunicaţiilor în masă, în cadrul căreia oamenii evitau televizorul în favoarea activităţilor sociale.

56. „Efectul de reţea” este efectul pe care-l are faptul că o persoană efectuează o anumită activitate asupra probabilităţii ca şi alte persoane să efectueze aceeaşi activitate.

57. Pentru mai multe informaţii despre investigaţia Marelui Juriu, vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei” care precedă discuţia.

58. Conform publicaţiei *Wall Street Journal*: „Conform unor documente analizate de *Wall Street Journal*, guvernul SUA a obţinut un tip controversat de hotărâre judecătorească secretă prin care compania Google Inc. şi micul furnizor de internet Sonic.net Inc.

erau obligate să predea informaţii din conturile de e-mail ale voluntarului Wikileaks Jacob Appelbaum […] Procesul Wikileaks a devenit un banc de probă pentru interpretarea legii în prima parte a anului acestuia, când Twitter a atacat în instanţă o hotărâre judecătorească de a preda arhivele conturilor mai multor susţinători Wiki-Leaks, inclusiv ale domnului Appelbaum […] Ordinul căuta adresele „internet protocol" sau IP ale dispozitivelor de pe care persoanele vizate se conectau la conturile lor. O adresă IP este im număr unic acordat unui aparat conectat la internet. Hotărârea cerea şi adresele de e-mail ale persoanelor care comunicau cu aceste conturi. Hotărârea a fost emisă sub sigiliu, dar Twitter a primit din partea curţii dreptul de a notifica abonaţii ale căror informaţii erau căutate […] Hotărârile judecătoreşti care au fost analizate de *Wall Street Journal* vizează acelaşi tip de informaţii cu cele pe care Twitter a fost somat să le predea. Hotărârea secretă pentru compania Google datează din 4 ianuarie şi cere uriaşului motor de căutare să predea adresa IP de pe care dl Appelbaum s-a conectat la contul său gmail.com şi adresele de e-mail şi adresele IP ale utilizatorilor cu care a comunicat începând cu data de 1 noiembrie 2009. Nu este clar dacă Google a atacat în instanţă hotărârea sau a predat documentele cerute. Hotărârea secretă pentru compania Sonic este datată 15 aprilie şi cere lui Sonic să predea acelaşi tip de informaţie despre contul de e-mail al domnului Appelbaum începând cu data de 1 noiembrie 2009. În 31 august, curtea a permis ca sigiliul să fie ridicat de pe hotărârea Sonic şi să trimită domnului Appelbaum o copie".

„Ordine secrete vizează e-mailurile", *Wall Street Journal*, 9 octombrie 2011: http://online.wsi.com/article/ZB1.000 l424052970203476804576613

284007315072.html (accesat în data de 11 octombrie 2012). Pentru mai multe detalii, vezi „Notă despre diversele încercări de a persecuta Wiki-Leaks şi pe cei asociaţi ei" care precedă discuţia.

59. „Wikileaks cere companiilor Google şi Facebook să desigileze citaţiile US", *Guardian*, 8 ianuarie 2011: http://www.guardian.co.uk/media/2011/ jan/08/wikileaks-calls-google-facebook-us-subpoenas (accesat în data de 16 octombrie 2012). Pentru mai multe detalii, vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei" care precedă discuţia.

60. Vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei" care precedă discuţia.

61. Pentru mai multe detalii, vezi site-ul Europe *versus* Facebook: http://www.europe-v-facebook.org/EN/Data Pool/data pool.html (accesat în data de 24 octombrie 2012).

62. O Scrisoare de Siguranţă Naţională sau SSN [„National Security Letter", NSL] este o scrisoare trimisă de o agenţie SUA prin care se cer „date fără conţinut" sau „metadate", cum ar fi arhive ale tranzacţiilor financiare, registre IP sau adrese de contact din e-mail. Oricine primeşte o SSN trebuie să predea informaţia cerută, altminteri va suferi urmări penale. O SSN nu are nevoie de autorizaţia unui tribunal, poate fi emisă direct de o agenţie federală. Din acest motiv este similară aşa-numitei „somaţii administrative" – un ordin în vederea predării de informaţii care are nevoie doar de monitorizare administrativă, nu şi juridică. Din acest motiv, se poate spune că SSN-urile încalcă protejările împotriva percheziţiei şi confiscării arbitrare ale Celui De-al Patrulea Amendament. SSN-urile conţin şi o clauză de păstrare

forţată a tăcerii, ceea ce înseamnă că este o infracţiune ca cineva care primeşte o SSN să vorbească despre ea cu altcineva. Din acest motiv, se poate spune că SSN-urile încalcă libertatea de expresie garantată de Primul Amendament. În procesul Doe *versus* Gonzales, clauza de păstrare forţată a tăcerii a fost declarată neconstituţională. Legea a fost schimbată pentru a acorda celor care primesc o SSN dreptul să o conteste în instanţă, lucru care a satisfăcut Curtea pentru cel De-al Doilea Circuit că folosirea lor nu mai este neconstituţională. SSN-urile continuă să fie criticate de activiştii pentru libertăţile civice şi contestate în instanţă.

Folosirea SSN-urilor a crescut în mod drastic după ce a fost aprobată legea PATRIOT Act în 2001. De obicei, cei care primesc SSN-uri sunt furnizori de servicii, cum e cazul ISP-urilor sau instituţiilor financiare. Arhivele cerute sunt în mod normal ale clienţilor celui care primeşte SSN-ul. Acesta nu poate informa clientul că arhivele sale au fost cerute. Deşi cei care primesc SSN-uri au dreptul de a le contesta în instanţă, clauza de păstrare forţată a tăcerii îl împiedică pe cel vizat să afle măcar de existenţa SSN-ului, aşadar îl împiedică să o conteste în instanţă. Pentru a înţelege cât de dificil de justificat este acest lucru, vezi o filmare a avocatului general adjunct al FBI încercând să răspundă la întrebarea lui Jacob Appelbaum, „Cum pot să mă duc la un judecător dacă partea terţă e obligată să păstreze tăcerea şi nu poate să-mi spună că sunt vizat de către voi?” Răspunsul ei îţi dă fiori: „Există unele momente când lucrurile astea sunt necesare”: http://youtu.be/dâuxoLDnmJU (poate fi găsit de asemenea, împreună cu material contextual, la Privacy SOS: http://privacysos.org/node/727).

Conform Electronic Frontier Foundation, „Dintre

toate puterile periculoase de supraveghere ale guvernului care au fost dezvoltate de USA PATRIOT Act, puterea pe care o are Scrisoarea de Siguranţă Naţională (SSN) după prevederile 18 U.S.C. § 2709, după cum a fost dezvăluit în Secţiunea 505 a legii PATRIOT, este una dintre cele mai înspăimântătoare şi invazive. Aceste scrisori, trimise furnizorilor de servicii de comunicaţii precum companiile de telefonie şi ISP-urile, permit FBI-ului să ceară în secret date despre comunicaţiile private şi activitatea de internet a oricăror cetăţeni americani, fără nicio monitorizare semnificativă sau vreo analiză premergătoare a unui organ juridic. Cei care primesc SSN-uri sunt supuşi unui ordin care le interzice să dezvăluie existenţa scrisorii colegilor de muncă, prietenilor sau măcar membrilor familiei, cu atât mai puţin publicului". Vezi: https://www.est.org/issues/national-security-letters. Vezi de asemenea colecţia de documente referitoate la Scrisoarea de Siguranţă Naţională a Electronic Frontier Foundation, publicate sub prevederile Legii Libertăţii Informaţiei: https://www.est.org/issues/foia/07656JDB (toate linkurile din această notă au fost accesate în data de 23 octombrie 2012).

63. Vezi mai sus, nota 41, despre „Primul Război Criptografic" al anilor '90.

64. Julian se referă la SSL/TLS, care este un algoritm criptografic încorporat acum ca standard în fiecare browser şi care este folosit pentru navigare secretă – de exemplu, când browserul este folosit pentru tranzacţii financiare pe internet.

65. Pentru unul dih multele exemple, vezi „Blackberry, Twitter probed în London riots", Bloomberg, 9 august 2011: http://www.bloomberg.com/ news/2011 – 08 – 09/blackberry-messages-probed-in-u-k-rioting-as-police-

say-looting-organized.html (accesat în data de 16 octombrie 2012).

66. De exemplu, un membru al grupării Lulzăec, care a scos la iveală puncte slabe ale practicilor de securitate ale Sony publicând date personale ale clienţilor Sony, a fost arestat după ce i-a fost aflată identitatea de pe site-ul proxy HideMyAss.com în urma unei hotărâri judecătoreşti în SUA. Vezi „Lulzsec hacker pleads guilty over Sony attack", BBC, 15 octombrie 2012: http://www.bbe.com/news/technology-19949624 (accesat în data de 15 octombrie 2012).

67. SOPA se referă la Stop Online Piracy Act (Legea Opririi Pirateriei Online). PIPA se referă la Protect Intellectual Property Act (Legea pentru Protecţia Drepturilor de Proprietate Intelectuală). Ambele sunt legi propuse în SUA care au căpătat o importanţă mondială în 2012. Ambele sunt expresii legislative clare ale dorinţei industriei de conţinut, reprezentată de Recording Industry Association of America [Asociaţia Industriei de înregistrări din

America], de a promulga în întreaga lume intrarea în vigoare a legilor proprietăţii intelectuale, iar asta într-o manieră cât se poate de dură, ca reacţie la distribuţia gratuită online de produse culturale. Ambele legi propuneau să se garanteze agenţiilor executive ale SUA puterea absolută şi universală de a cenzura internetul, ceea ce ameninţa să „rupă internetula. Ambele au fost primite cu indignare de către părţi substanţiale ale comunităţii internaţionale online şi au provocat o reacţie puternică din partea actorilor industriali ale căror interese se bazează pe un internet liber şi deschis.

La începutul lui 2012, Reddit, Wikipedia şi alte câteva mii de site-uri şi-au închis serviciile în semn de

protest împotriva acestor legi, instigând la grele presiuni publice asupra reprezentanţilor publici. Alţi furnizori de servicii online, cum ar fi Google, au încurajat petiţiile. În consecinţă, ambele legi au fost suspendate până la reconsiderarea şi discutarea faptului dacă reprezintă cea mai bună abordare a problemei proprietăţii intelectuale în domeniul online. Episodul este văzut ca prima descoperire semnificativă şi afirmare a puterii eficiente de lobby deţinute asupra Congresului de către industria internetului.

68. Vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei" care precedă discuţia.

69. ACTA se referă la Anti-Counterfeiting Trade Agreement [Acordul Comercial de Combatere a Contrafacerii]. Este un tratat multilateral internaţional, negociat în secret timp de mai mulţi ani, condus de către Statele Unite şi Japonia, care instituie, în parte, obligaţii noi şi aspre în vederea protejării proprietăţii intelectuale.

Unele ciorne iniţiale ale ACTA au fost dezvăluite publicului în 2008, după ce au fost scurse către Wikileaks, provocând exclamaţii generale de dezaprobare din partea activiştilor pentru cultura liberă şi a susţinătorilor online. Vezi secţiunea ACTA de pe Wikileaks: http://wikileaks.org/wiki/ Category: ACTA.

Telegramele diplomatice ale SUA distribuite de către Wikileaks organizaţiei La Quadrature Du Net la începutul lui 2011 au arătat că ACTA a fost negociată în secret în mod explicit pentru a se accelera crearea unor reguli extreme de sancţionare a IP-urilor, care ar putea apoi fi impuse cu forţa unor ţări mai sărace care au fost excluse din acord. Vezi „Wikileaks Cables Shine Light on ACTA History", La Quadrature Du Net, 3 februarie 2011:

http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history (accesat în data de 23 octombrie 2012).

În iulie 2012, după o campanie condusă de site-ul La Quadrature Du Net şi Jérémie Zimmermann, ACTA a fost învinsă în Parlamentul European.

70. M.A.I.D. (Mutually) Assured Information Destruction [Distrugere de Informaţii Asigurata Reciproc] este „un program care furnizează servicii de «key escrow» cu acţionare de la distanţă, temporizator şi autentificare verificabilă şi opţiunea de codificare de urgenţă. Distruge automat cifrele criptografice după ce este depăşit un prag temporal configurabil de către utilizator”: https://www.noise-bridge.net/wiki/M. A.I.D.

Unele legi, ca Regulation of Investigatory Powers Act [Legea Reglementării Puterilor de Investigare] din 2000, sau RÂPA, fac ca Regatul Unit să fie un regim destul de ostil criptografiei. Sub legea RÂPA, indivizii pot fi obligaţi să descifreze date sau să predea parola la ordinul unui ofiţer al poliţiei. Nu e necesară monitorizarea de către un organ judecătoresc. Refuzul poate conduce la acuzaţii de infracţionalitate. Într-un proces, dacă acuzatul/acuzata pretinde că a uitat parola, are loc o inversare a sarcinii de a aduce dovezi. Pentru a evita să fie condamnat (a), acuzatul/acuzata trebuie să dovedească că a uitat parola. Lucrul acesta, spun criticii legii, constituie o prezumţie de vinovăţie. Prin comparaţie, deşi au avut loc multe litigii referitoare la aceleaşi probleme şi în Statele Unite, iar situaţia e departe de a fi ideală, în circumstanţe similare au fost repurtate mai multe succese prin invocarea Primului sau a Celui De-al Patrulea Amendament. Vezi articolul „Freedom from Suspicion, Surveillance Reform for a Digital Age”, publicat de JUSTICE, 4 noiembrie 2011,

disponibil la: http://www.justice.org.uk/ resources.php/305/freedom-ffom-suspicion.

Pentru mai multe informaţii despre sistemul de fişiere Rubberhose, vezi „The Idiot Savants* Guide to Rubberhose”, Suelette Dreyfus: http://marutukku.org/current/src/doc/maruguide/îl.html (toate linkurile au fost accesate în data de 24 octombrie 2012).

71. O arhivă a vechii liste de e-mailuri Cypherpunk poate fi descărcată la: http://cryptome.org/cpunks/cpunks-92 – 98.zip.

Tim May a fost membru fondator al listei de e-mailuri Cypherpunk. Vezi *Cyphemomicon-ul* său, un FAC despre istoria şi filosofia cypherpunk: http://www.cypherpunks.to/fac/cypher-nomicron/cypherno micon.html (ambele linkuri au fost accesate în data de 24 octombrie 2012).

72. *„Proposed US ACTA plurilateral intellectual property trade agreement (2007)”*, Wikileaks, 22 mai 2008: http://wikileaks.org/wiki/Proposed US ACTA multilateral intellectual property trade agreement %282007%29 (accesat în data de 21 octombrie 2012).

73. *„Massive Takedown of Anti-Scientology Videos on YouTube”*, Electronic Frontier Foundation, 5 septembrie 2008: https://www.est.org/deeplinks/ 2008/09/massive-takedown-anti-scientology-videos-youtube (accesat în data de 16 octombrie 2012).

74. *JEU India Free Trade Agreement draji, 24 Feb 2009”*, Wikileaks, 23 iunie 2009: http://wikileaks.org/wiki/EU-India Free Trade Agreement draft, 24 Feb 2009 (accesat în data de 21 octombrie 2012).

75. Peer-to-peer, sau P_2P, se referă la o reţea în care fiecare computer poate funcţiona în calitate de client sau

de server pentru toate celelalte (fiecare computer poate atât să trimită, cât şi să primească informaţie), permiţând distribuirea rapidă a unor conţinuturi de date cum ar fi muzică, înregistrări video sau orice fel de informaţie digitală.

76. Cloud computing se referă la o situaţie în care multe dintre funcţiile îndeplinite în mod normal de un computer, cum ar fi stocarea de date (inclusiv datele de utilizator pentru diverse aplicaţii), găzduirea şi administrarea de software şi furnizarea şi procesarea energiei cu care funcţionează software-ul, se face la distanţă, departe de computerul ca atare, „în nor" [*cloud* se traduce prin *nor*\ – de regulă de către companii care oferă servicii de cloud computing prin internet. În loc să aibă nevoie de un computer complet, tot ceea ce îi trebuie utilizatorului este un aparat care poate accesa internetul, iar restul este servit utilizatorului prin internet. Metafora „în nor" ascunde faptul că toate datele şi metadatele utilizatorului se află de fapt într-un computer undeva într-un centru de date, cel mai probabil controlat de o companie mare, cum ar fi Amazon, şi în timp ce utilizatorii nu mai au controlul complet asupra lor, îl are altcineva.

77. Vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi era care precedă discuţia.

78. DIASPORA este o reţea de socializare care permite fiecărui utilizator să funcţioneze ca propriul său server prin instalarea software-ului DIASPORA, care îi permite să păstreze controlul asupra datelor sale. A fost creat ca o alternativă la Facebook care permite confidenţialitatea. Este nonprofit şi este deţinut de utilizator: http://diasporaproject.org.

79. Primul Napster (1999 – 2001) a fost un serviciu

inovativ de tipul peerto-peer pentru distribuţia de muzică. A avut o popularitate enormă, dar a fost închis repede prin acţiuni juridice intentate de Asociaţia Industriei de înregistrări din America din cauza încălcării drepturilor de autor. După faliment, numele Napster a fost cumpărat şi folosit pentru *un* alt magazin Online de vânzare de muzică.

80. Vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei” care precedă discuţia.

81. Benjamin Bayart este preşedintele companiei French Data NetWork, cel mai vechi ISP activ din Franţa şi un susţinător al neutralităţii internetului şi al software-ului liber. Vezi pagina sa de Wikipedia (în franceză): http://fr. wikipcclia.org/wiki/Benjamin Bayart (accesată în data de 15 octombrie 2012).

82. Larry Lessig este un academician şi activist american cunoscut mai cu seamă pentru viziunile sale despre drepturile de autor şi cultura liberă. Blogul său se află la: http://lessig. tumbir.com (accesat în data de 15 octombrie 2012).

83. Există multe informaţii fascinante referitoare la această chestiune în telegramele diplomatice ale SUA publicate de Wikileaks. Pentru o discuţie interesantă, vezi următoarele telegrame (după ID-ul de referinţă al telegramei, toate linkurile au fost accesate în data de 24 octombrie 2012): 07BEIRUT1301: http://wikileaks.org/cable/2007/08/07BEIRUT 1301 Jitml 08BEIRUT490: http://wilrileaks.org/cable/2008/04/08BEIRUT490.html 08BEIRUT505: http://wikileaks.org/cable/2008/04/08BEIRUT505.html 08BEIRUT523: http://wilrileaks.org/cable/2008/04/08BEIRUT523.htmL

84. Vezi ID-ul de referinţă al telegramei 10MOSCOW228, Wikileaks: http://wikileaks.org/cable/2010/02/10MOSCOW228.html (accesat în data de 24 octombrie 2012).

85. Pentru mai multe informaţii despre uciderea fără proces a cetăţenilor americani Anwar al-Awlaki şi a fiului său, Abdulrahman al-Awlaki, vezi Glenn Greenwald, „The duc-process-free assassination of U.S. citizens is now reality", Salon, 30 septembrie 2011: http://www.salon.com/2011/09/30/ awlaki 6. Şi „*The killing of Awlakis 16-year-old son*", Salon, 20 octombrie 2011: http://www.salon.com/2011/10/20/the killing of awlakis 16 year old son.

„Este pur şi simplu imposibil să ne imaginăm o desconsiderare mai violentă a mecanismelor fundamentale ale republicii decât dezvoltarea unei agenţii a ramurii executive, secrete, care nu poate fi deloc trasă la răspundere şi care colectează în acelaşi timp informaţii despre toţi cetăţenii şi apoi aplică o „matrice de dispoziţie" pentru a determina ce pedeapsă trebuie să se stabilească. Aceasta este clasica distopie politică adusă la realitate" – Glenn Greenwald, „Obama moves to make the War on Terror permanent", *Guardian*, 24 octombrie 2012: http://www.guardian.co.uk/commentistree/2012/ oct/24/obama-terrorism-kill-list (toate linkurile au fost accesate în data de 24 octombrie 2012).

86. Pentru informaţii ulterioare, vă rugăm să consultaţi „The Anonymity Bibliography, Selected Papers în Anonymity", ediţie îngrijită de Roger Dingledine şi Nick Mathewson: http://ffeehaven.net/anonbib (accesat în data de 24 octombrie 2012).

Moneda chaumiană este emisă central, dar foloseşte criptografia pentru a asigura tranzacţii anonime. Moneda

chaumiană se deosebeşte de Bitcoin, altă monedă electronică discutată pe larg mai jos, în cazul căreia toate tranzacţiile sunt publice, dar moneda nu are o autoritate centrală.

87. Pentru mai multe informaţii despre blocada bancară împotriva Wikileaks, vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi era care precedă discuţia.

88. Julian se referă aici la planurile Regatului Unit de a creşte folosirea dispozitivelor electronice de urmărire. Vezi „Over 100.000 offenders to be electronically tagged", *Guardian*, 25 martie 2012: http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice (accesat în data de 22 octombrie 2012).

În momentul discuţiei, Julian se afla în arest la domiciliu, în aşteptarea rezultatului procesului său de extrădare. După închiderea sa în izolare, fără acuzare, în decembrie 2010, detenţia lui Julian a fost transformată în arest domiciliar după ce a plătit o sumă de 300.000 de lire sterline pentru eliberarea pe cauţiune. O condiţie a eliberării sale a fost consemnarea la o anumită adresă într-un anumit interval temporar, iar acest regim a fost impus de un dispozitiv electronic de urmărire fixat în jurul gleznei sale, administrat de o firmă privată de securitate contractată de guvernul Regatului Unit. Mişcările lui Julian erau controlate în aşa măsură încât era constrâns să raporteze zilnic poliţiei, la o anumită oră, timp de peste 550 de zile. În momentul publicării celor de faţă, Julian se află consemnat la Ambasada Ecuadorului din Londra, care este înconjurată în fiecare moment de Poliţia Metropolitană a Londrei. În iunie 2012, Julian a intrat în ambasadă căutând azil politic din cauza persecuţiei Statelor Unite şi a aliaţilor săi. A primit azil în august

2012.

89. „Is CC A Trying to Take Over the World?”, American Civil Liberties Union, 21 februarie 2012: http://www.aclu.org/blog/prisoners-rights/ceatrying-take-over-world.

„Passing House Bill will worsen already pressing civil rights issue”, AN-NARBOR.com, 2 august 2012: http://armarbor.com/news/opinion/ passing-house-bill-will-worsen-already-pressing-civil-rights-issue.

Vezi, de asemenea, „Goldman Sachs to invest $9.bun în New York înmate rehabilitation”, *Guardian*, 2 august 2012: http://www.guardian.co.uk/ society/2012/aug/02/goldman-sachs-invest-new-york-jail (toate linkurile au fost accesate în data de 24 octombrie 2012).

90. Bitcoin (http://bitcoin.org) este prima implementare care a avut succes a unui concept clasic al mişcării cypherpunk: moneda digitală criptografică. Moneda Bitcoin este discutată pe larg mai jos, dar o explicaţie introductivă excelentă despre tehnologia şi filosofia din spatele ei poate fi găsită la „Understanding Bitcoin”, Al Jazeera, 9 iunie 2012: http://www.aljazeera.com/îndrepth/opi-nion/2012/05/20125 309437931677.html (accesat la data de 22 octombrie 2012).

91. E-gold a fost o monedă electronică şi o afacere care a început în 1996. Pro – prietarii au fost acuzaţi de Departamentul de Justiţie al SUA de „complot pentru spălare de bani”. Au pledat vinovaţi şi au primit pedepse cu suspendare, arest domiciliar şi muncă în favoarea comunităţii. Judecătorul care a dat sentinţa a spus că meritau sentinţe uşoare din cauză că nu intenţionaseră să facă activităţi ilegale. Vezi „Bullion and Bandits: The

Improbable rise and Fall of E-Gold", *Wired*» 9 iunie 2009: http://www.wired.com/threatlevel/2009/06/e-gold (accesat în data de 22 octombrie 2012).

92. Înaintea internetului, reţeaua X.25 era cea mai mare reţea globală pentru schimbul de date, existând în paralel cu reţeaua de telefonie. Contorizarea pe X.25 se baza pe cantitatea de date trimise şi primite, nu pe lungimea unei conexiuni, ca în cazul reţelei de telefonie. Porţile de acces (aşa-numitele PADS) permiteau conectarea la reţeaua X.25 de la o reţea de telefonie prin intermediul unui modern sau al unor cuplaje acustice. Pentru mai multe detalii vezi Wikipedia: http://en.wikipedia. Org/wiki/X.25 (accesat în data de 24 octombrie 2012).

93. David Chaum este criptograf şi inventator de protocoale criptografice. Este un pionier al tehnologiilor monetare digitale şi a elaborat elash, una dintre primele monede electronice criptate şi anonime.

94. Pentru a vedea efectul pe care l-au avut recenziile negative din presă vezi, „Bitcoin implodes, falls more than 90 percent from June peak", arstechnica, 18 octombrie 2011: http://arstechnica.com/techpolicy/2011/10/ bitcoin-implodes-down-more-than-90-percent-from-junepeak (accesat în data de 22 octombrie 2012).

95. Vezi, de exemplu, „7 Tie Underground Website Where You Can Buy Any Drug Imaginable", *Gawker*, 1 iunie 2011: http://gawker.com/5805928/ the-underground-website-where-you-can-buy-any-drug-imaginable (accesat în data de 22 octombrie 2012).

96. În ultimii ani, Lawrence Lessig a adăugat activităţii sale timpurii din domeniul copyrightului şi al culturii (care poate fi văzută, de pildă, în cartea sa *Free Culture*, 2004) un interes faţă de procesul de corupere a democraţiei americane prin intermediul lobby-ului

congresional. Vezi The Lessig Wiki: http://wiki. lessig.org.

97. Asociaţia Corecţional Peace Officers din California este un grup de interese din California care face, în mod curent, donaţii de câte şapte cifre în timpul alegerilor statale, deşi nu este, an de an, cea mai mare donatoare de campanie. Vezi „California reelin", *The eeconomist** *17* martie 2011: http://www.economist.com/node/18359882. Şi „The Golden States Iron Bars", Reason, iulie 2011: http://reason.com/archives/2011/06/23/the-goldenstates-iron-bars. Vezi şi pagina Asociaţiei Corecţional Peace Officers din California pe site-ul Follow The Money al National Institute for Money în State Politics: http://www.followthemoney.org/database/topcontributor. phtml? u = 3286 & y = O (toate linkurile au fost accesate în data de 22 octombrie 2012).

98. Hanz von Foerster (1911 – 2002) a fost un cercetător american de origine austriacă şi arhitect al ciberneticii. Aşa-numitul său „imperativ etic" sau motto era: „Acţionează tot timpul în aşa fel încât să sporeşti numărul opţiunilor" sau, în germană: „Handle stets so, daß die Anzahl der Wahimöglichkeiten größei wird".

99. Jacob atribuie această observaţie lui John Gilmore. [În text, And everybody else who is struggling to get along isn't acknowledged as even having bits that are worthflipping in thefirst place. – n.tr.]

100. Pentru mai multe informaţii despre hărţuirea lui Jacob şi a altor persoane asociate cu Wikileaks, vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei" care precedă discuţia.

101. Isaac Mao este un blogger, creator de sotfware şi investitor din China. Este cofondator al site-ului CNB – log.org şi membru al consiliului de conducere al

Proiectului Tor.

102. Vezi pagina de Wikileaks despre Nadhmi Auchi: http://wikileaks.org/ wiki/Nadhmi Auchi (accesat în data de 24 octombrie 2012).

103. Articolele pot fi găsite pe site-ul Wikileaks, aici: http://wikileaks.org/ wiki/Eight stories on Obama linked billionaire Nadhmi Auchi cenzored from the Guardian, Observer, Telegraph and New Statesman (accesat în data de 24 octombrie 2012).

104. În linii mari, atât http://cables. mrkva.eu/, cât şi http://cablegatesearch.net furnizează modalităţi excelente de a compara versiunile revizuite şi pe cele complete ale telegramelor, pentru a vedea ce au eliminat partenerii media ai Wikileaks.

105. „Qaddafis Son Is Bisexual and Other Things the *New York Times* Doesn't Want You to Know", *Gawker*, 16 septembrie 2011: http://gawker.com/5840809/qaddafis-son-is-bisexual-and-other-things-the-new-yorktimes-doesnt-want-you-to-know-about.

Exemplul citat se referă la ID-ul de referinţă al telegramei 06TRIPOLI198, Wikileaks: https://wikileaks.org/cable/2006/05/06TRIPOLI 198.html.

Părţile redactate pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, redactările fiind subliniate în roz: http://www.cablegatesearch.net/cable.php? id = 06TRIPOLI 198 & version = 1291757400 (toate linkurile au fost accesate în data de 22 octombrie 2012).

106. Pentru telegrama originală vezi telegrama cu ID-ul de referinţă 10STA-TE17263, la Wikileaks: http://wikileaks.org/cable/2010/02/10STA-TE17263.html.

Pentru articolul din *New York Times*, vezi „Iran Fortifies Its Arsenal With the Aid of North Korea", *New*

York Times, 29 noiembrie 2010: http://www.nytimes.com/2010/11 /29/world/middle-east/29 missiles.html? r = O. Aceeaşi telegramă a fost folosită de către David Leigh de la *The Guardian* pentru articolul său: „Wikileaks cables expose Pakistan nuclear fears", *Guardian*, 30 noiembrie 2010: http://www.guardian.co.uk/world/2010/ nov/30/wikileaks-cables-pakistan-nuclear-fears. Versiunea revizuită a telegramei, publicată de *The Guardian*, fără un număr de referinţă, e redusă la doar două paragrafe referitoare la Pakistan. „US embassy cables: XXXXXXXXXXXX", *Guardian*, 30 noiembrie 2010: http://www.guardian.co.uk/world/us-embassy-cables-documents/250573.

Pe site-ul Cablegatesearch se poate vedea în ce măsură textul a fost revizuit, aici găsindu-se arhiva revizuirilor, părţile redactate ale documentului fiind aproape în întregime subliniate în roz: http://www.cablegate-search.net/ cable.php? id = 10STATE17263 & version = 129 l486260 (toate linkurile au fost accesate în data de 22 octombrie 2012).

107. Pentru telegrama originală vezi telegrama cu ID-ul de referinţă 08KYIV2414, la site-ul Wikileaks: http://wikileaks.org/cable/2008/12/ 08KYIV24 l4.html.

Pentru versiunea redactată de *The Guardian*, vezi „US embassy cables: Gas supplies linked to Russian mafia", 1 decembrie 2010: http://www.guardian. co.uk/world/us-embassy-cables-documents/182121? INTEMP = SRCH. Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, editările fiind subliniate în roz: http://www.cablegatesearch.net/ cable.php? id = 08KYIV24 l4 & version = 1291255260 (toate linkurile au fost accesate în data de 22 octombrie

2012).

108. Pentru telegrama originală vezi telegrama cu ID-ul de referinţă 10AS-TANA72, la Wikileaks: http://wikileaks.org/cable/2010/01/10ASTA-NA72.html.

Pentru versiunea redactată de *The Guardian*, vezi „US embassy cables: Kazakhstan – the big four", *Guardian*, 29 noiembrie 2010: http://www.guardian. co.uk/world/us-embassy-cables-documents/245167? INTEMP = SRCH.

Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, redactările fiind subliniate în roz: http://www.cablegatesearch.net/cable.php? id = 10ASTANA72 & version = 1291113360 (toate linkurile au fost accesate în data de 22 octombrie 2012).

109. Vezi, de pildă, telegrama cu ID-ul de referinţă 09TRIPOLI413, despre companiile europene de energie cu sedii în Libia. Reprezentarea grafică de pe site-ul Cablegatesearch, care pune în roz editările făcute de *The Guardian*, arată că publicaţia a scos toate referirile făcute la numele companiilor energetice sau la directorii acestora, în afară de cele privitoare la Gazprom, compania rusească de energie. Deşi o parte din conţinut este oarecum justificator pentru companiile europene, redactările sunt minuţioase, iar versiunea redactată prezintă o imagine complet diferită: http://www.cablegate-search.net/cable.php? id = 09TRIPOLI413 & version = 1296509820 (accesat în data de 22 octombrie 2012).

110. Telegrama originală menţionată în acest exemplu conţinea 5 226 de cuvinte. Versiunea editată publicată în *The Guardian* conţinea doar 1 406 de cuvinte. Pentru telegrama originală vezi telegrama cu ID-ul de referinţă 05SO-FIA1207, pe site-ul Wikileaks: http://wikileaks.org/cable/2005/07/ 05SOFIA1207.html.

Pentru versiunea editată de *The Guardian*, vezi „US

embassy cables: Organised crime în Bulgaria", 1 decembrie 2010: http://www.guardian.co.uk/ world/us-embassy-cables-documents/36013.

Pentru articolul din *The Guardian* bazat pe această telegramă, vezi „Wikileaks cables: Russian government «using mafia for its dirty work»", *Guardian*, 1 decembrie 2010: http://www.guardian.co.uk/world/2010/ dec/01 /wikileaks-cable-spain-russian-mafia.

Pe site-ul Cablegatesearch se poate vedea în ce măsură textul a fost revizuit, aici găsindu-se arhiva revizuirilor, editările fiind subliniate în roz: http://www.cablegatesearch.net/cable.php? id = 05SOFIAl207 & version = 1291757400.

Exemplul bulgar este discutat de publicaţia *Bivol*, partener media al Wikileaks, în „Unedited cable from Sofia shows the total invasion of the state by organized crime (Update: Cable Comparison)", WL Central, 18 martie 2011: http://wlcentral.org/node/1480.

De asemenea, vezi „The Guardian: Redacting, cenzoring or lying?", WL Central, 19 martie 2012: http://wlcentral.org/node/1490.

Interesant, pe subiectul celor două articole ale WL Central, este comentariul jurnalistului David Leigh de la *The Guardian* şi răspunsurile la acesta. (Toate linkurile au fost accesate în data de 22 octombrie 2012.)

111. Exemplul acesta se referă la telegrama cu ID-ul de referinţă 09BER-LIN1108. Editările pot fi urmărite pe site-ul Cablegatesearch, care arată arhiva revizuirilor, editările fiind subliniate în roz: http://www.cablegatesearch.net/cable.php? id = 09BERLIN 1108 & version = 1291380660 (accesat la data de 22 octombrie 2012).

112. Pentru mai multe exemple, vezi site-ul

cabledrum: www. cabledrum.net/ pages/cenzorship.php

113. „Interceptarea telecomunicaţiilor. Preşedinţia a furnizat informaţii despre situaţia actuală [...] A atras atenţia în legătură cu reacţia negativă pe care chestiunea a primit-o din partea mass-media [...] În aceste circumstanţe, preşedinţia a recunoscut că progresul în această chestiune este foarte lent [...] Mai multe delegaţii şi-au exprimat reţinerea în ceea ce priveşte pregătirea unei declaraţii de presă, atrăgând atenţia că acest lucru ar putea provoca o reacţie în lanţ şi o continuare a reacţiei negative în mass-media. Deşi a declarat că nu şi-a schimbat poziţia, comisia a informat delegaţiile că un mod de a ieşi din impas ar fi să urmeze o strategie similară cu cea urmată în abordarea chestiunii pornografiei infantile pe internet. Deşi acesta a fost un subiect diferit, el are şi tangenţe cu chestiunea interceptării" – „European Commission, Police Co-operation Working Group meeting on interception of télécommunications", 13 – 14 octombrie 1999. Vezi documentul complet la adresa: http://www.quintessenz.at /doqs/000100002292/1999 10 13 – Police%20 Cooperation%20 Working%20 Group%20 mixed%20 committee%20 meeting.pdf (accesat la data de 24 octombrie 2012).

114. Vezi „Notă despre diversele încercări de a persecuta Wikileaks şi pe cei asociaţi ei" care precedă discuţia.

115. Jacob se referă la procesul Gilmore *versus* Gonzales, nr. 435 R3 d 1125 (al 9-lea Cir. 2006). John Gilmore, unul dintre primii cypherpunks, a ajuns cu un proces până la Curtea Supremă a SUA pentru a scoate la iveală conţinutul unei legi secrete – o directivă de securitate – ce restricţiona dreptul cetăţenilor de a călători cu avionul fără a se legitima. Pe lângă atacarea

constituţionalităţii unei astfel de prevederi, Gilmore ataca faptul că prevederea ca atare este secretă şi nu putea fi dezvăluită, deşi are efecte constrângătoare asupra cetăţenilor SUA. Curtea a consultat în secret directiva de securitate şi a decis împotriva lui Gilmore în privinţa constituţionalităţii directivei. Cu toate acestea, conţinutul legii nu a fost niciodată dezvăluit pe perioada deliberărilor. Vezi Gilmore *versus* Gonzales la Papers Please.org: http://papersplease.org/gilmore/facts.html (accesat în data de 22 octombrie 2012).

116. Christiania este o zonă autodeclarată, care se autoguvernează în Copenhaga, Danemarca. Fostă cazarmă militară, a fost ocupată în anii 1970 de o comunitate colectivist/anarhistă. Şi-a creat un statut juridic unic în Danemarca.

117. Principiul neutralităţii reţelei implică împiedicarea ISP-urilor (prin lege, se cere de obicei) de a restricţiona accesul utilizatorilor lor la reţelele care participă la internet, inclusiv restricţionarea conţinutului. Vezi pagina Fundaţiei Electronic Frontier despre subiectul neutralităţii reţelei: https://www.est.org/issues/net-neutrality (accesat în data de 24 octombrie 2012).

118. „Blocking Wikileaks e-mails trips up Bradley Manning prosecution", Politico, 15 martie 2012: http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-117573.html (accesat în data de 21 octombrie 2012).

119. Pentru mai multe informaţii despre Wau Holland, vezi Wau Holland Stiftung: http://www.waulând.de

120. „Stasi still în charge of Stasi files", Wikileaks, 4 octombrie 2007: http://www.wikileaks.org/wiki/Stasi still în charge of Stasi files (accesat în data de 22 octombrie

2012).

121. „lată ce puteţi face ca să schimbaţi lumea, chiar acum, pentru a o face mai bună. Luaţi toţi banii pe care-i cheltuim pe armament şi apărare în fiecare an şi cheltuiţi-i în loc pe hrănirea, îmbrăcarea şi educarea săracilor lumii acesteia, lucru pe care [banii, n.tr.] l-ar face de mai multe ori, fără să excludă un singur om, şi am putea explora spaţiul, împreună, atât cel cunoscut, cât şi cel necunoscut, pentru totdeauna, în pace” – Bill Hicks. Pentru a viziona înregistrarea video, vezi „Bill Hicks-Positive Drugs Story”: http://youtu. be/vXllvW38 cHA (accesat la data de 24 octombrie 2012).

122. Legea Sarbanes-Oxiey din 2002 este o lege aprobată în SUA ca răspuns la scandalurile corporatiste şi de contabilitate ale Enron, Tyco International, Adelphia, Peregrine Systems şi Worldlom. Legea urmărea eliminarea practicilor corupte care au dus la aceste crize. Paragraful 1107 al acestei legi, codificat USC 1513 (e), stabileşte ca infracţiune orice încercare de a sancţiona denunţătorii.

123. Evgeny Morozov (2011), The Net Delusion: The Dark Side of Internet Freedonty Public Affairs.

124. Pentru informaţii despre software-ul liber, vezi „The Free Software Definition”, pe site-ul sistemului de operare GNU: https://www.gnu.org/philosophy/free-sw.html.

Hardware cu sursă deschisă înseamnă un tip de hardware care nu este îngreunat de brevete de proprietate, care este construit la standarde libere, unde nu există legi împotriva ingineriei inverse sau a manipulării (nu există legi de tipul „anti-sustragere”) şi unde principiile concepţiei, instrucţiunile şi planul sunt accesibile, astfel încât oricine le are şi are resursele necesare în acest sens să poată crea un duplicat.

Pentru mai multe informaţii despre hardware-ul cu sursă deschisă, vezi „Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DIY a, EHSM: http://ehsm.eu. Vezi şi „Open-source hardware” pe Wikipedia: https://en.wikipedia.org/wiki/Open-source hardware (toate linkurile au fost accesate în data de 24 octombrie 2012).

125. Vezi filmarea introductivă despre imprimanta 3D RepRap, care funcţionează pe principiul hardware-ului liber şi cu sursă deschisă: http://vimeo.com/5202148 (accesat în data de 24 octombrie 2012).

126. Fraza „Be the trouble you want to see in the world” [„Fii tulburarea pe care vrei să o vezi în lume”] este preluată din „A Softer World”, o publicaţie fotografică online comică: http://www.asofterworld.com/index.php? id = 189 (accesat în data de 24 octombrie 2012).

127. Pentru a studia mai departe oricare dintre problemele ridicate în timpul conversaţiei, Jacob recomandă următoarele două resurse bibliografice: „The Anonymity Bibliography, Selected Papers în Anonymity”, ediţie îngrijită de Roger Dingledine şi Nick Mathewson: http://freehaven.net/anonbib. „The Cenzorship Bibliography, Selected Papers în Cenzorship”, ediţie îngrijită de Philipp Winter: www.ce. kau.se/philwint/cenzorbib (ambele linkuri au fost accesate în data de 24 octombrie 2012).

128. Această notă este lăsată intenţionat goală.

129. Nawaat.org este un blog colectiv independent, lansat în 2004, în Tunisia: http://nawaat.org/portail. Tunileaks a fost lansat de către Nawaat în luna noiembrie a anului 2010, cu publicarea unor telegrame referitoare la Tunisia, preluate de la Wikileaks: https://tunileaks. appspot.com.

Pentru mai multe informaţii despre Tunileaks şi despre eforturile guvernului Ben-Ali împotriva sa, vezi „Tunisia: Cenzorship Continues as Wikileaks Cables Make the Rounds”, Global Voices Avocacy, 7 decembrie 2010: http://avocacy. globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds (toate linkurile au fost accesate în data de 24 octombrie 2012).